НУЗ "Узловая больница
на ст. Стерлитамак
ОАО "РЖД"

**НЕГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ «УЗЛОВАЯ БОЛЬНИЦА
НА СТАНЦИИ СТЕРЛИТАМАК ОАО «РЖД»**

П Р И К А З

«21» 07 2017 г. № 183/1

Об утверждении Положения об обработке и защите персональных данных

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», п р и к а з ы в а ю:

1. Утвердить Положение об обработке и защите персональных данных НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД».
2. Грихно Л.И. - заведующей терапевтическим отделением:

организовать изучение Положения со всеми категориями подчиненных должностных лиц, допущенными к обработке персональных данных;

организовать обработку и защиту персональных данных в соответствии с настоящим Положением.

3. На Ильину Н.А. - заместителя главного врача по клинико-экспертной работе возложить контроль за исполнением настоящего приказа.
4. Приказ довести до сотрудников НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», в части касающейся.

Главный врач Ю.В. Саидгалина

Ознакомлены
Ильина Н.А.
Грихно Л.И.

НУЗ "Узловая больница

на ст. Стерлитамак

ОАО "РЖД"

УТВЕРЖДЕНО
приказом Главного врача
НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД»
от «21» ___июля___2017 г. № 183/1

ПОЛОЖЕНИЕ

об обработке и защите персональных данных, обрабатываемых в информационных системах персональных данных

НУЗ «Узловая больница на ст. Стерлитамак

ОАО «РЖД»

Оглавление

I. Общие положения

1. Настоящее Положение, разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. №687 и «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. №1119, иными нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных, а также с нормативными документами ОАО «РЖД», определяет основные правила обработки и защиты в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» персональных данных пользователей услуг, контрагентов и иных субъектов персональных данных.

2. НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» является оператором, самостоятельно или совместно с другими лицами организующим и (или) осуществляющим обработку персональных данных субъектов персональных данных в целях, определенных в Политике. Обработка персональных данных, не отвечающая целям обработки, запрещается.

3. Настоящее Положение распространяются в том числе на случаи, когда НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» выступает лицом, осуществляющим обработку персональных данных по поручению стороннего оператора. Дополнительные условия по обработке и защите персональных данных указываются в договоре между НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» и сторонним оператором.

4. В настоящем Положении используются следующие понятия и термины:

1) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

2) автоматизированное рабочее место - рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций;

3) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

4) вымарывание персональных данных - действия, исключающие дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе;

5) допуск к обработке персональных данных - процедура оформления права на доступ к персональным данным;

6) доступ к персональным данным - возможность обработки персональных данных;

7) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; 8) контрагент

- юридическое или физическое лицо, с которым НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» состоит в договорных отношениях или планирует вступить в договорные отношения;

9) материальный носитель - бумажный или машинный носитель информации, предназначенный для фиксирования, передачи и хранения персональных данных;

10) машинный носитель - материальный носитель информации, предназначенный для записи и воспроизведения информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами (внутренние жесткие диски, флэш-накопители, внешние жесткие диски, CD-диски и иные устройства);

11) неавтоматизированная обработка персональных данных - обработка персональных данных, осуществляемая при непосредственном участии человека без использования средств вычислительной техники;

12) несъемный машинный носитель - машинный носитель, встроенный в корпус средства вычислительной техники, используемый для хранения и обработки информации (внутренние жесткие диски и иные устройства);

13) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

14) обработка персональных данных-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 (в том числе вымарывание), уничтожение персональных данных;

15) передача персональных данных - любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств, представляющих собой доступ, распространение, предоставление персональных данных;

16) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

17) пользователи услуг НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» - пациенты, работники ОАО «РЖД», либо иные физические или юридические лица, пользующиеся услугами, оказываемыми НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД»;

18) смешанная обработка персональных данных - обработка персональных данных, осуществляемая как неавтоматизированным, так и автоматизированным способами;

19) средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

20) субъекты персональных данных - пользователи услуг, контрагенты, а также иные лица, чьи персональные данные стали известны НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» при осуществлении своей деятельности;

21) съемный машинный носитель - машинный носитель, используемый для хранения информации вне ПЭВМ (флэш-накопители, внешние жесткие диски, CD-диски и иные устройства);

22) удаление персональных данных - действия, в результате которых становится невозможным ознакомиться с содержанием персональных данных в информационной системе или на материальном носителе информации;

23) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе и (или) в результате которых уничтожаются материальные носители персональных данных;

24) уполномоченные работники - работники НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», имеющие допуск к персональным данным субъектов персональных данных.

II. Правила обработки персональных данных в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД»

5. Обработка персональных данных субъектов персональных данных в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» должна осуществляться с соблюдением законодательства Российской Федерации и нормативных документов НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» в области обработки и защиты персональных данных.

6. При определении содержания и объема обрабатываемых персональных данных необходимо руководствоваться принципом достаточности по отношению к целям обработки персональных данных при исполнении своих обязательств перед субъектами персональных данных. Состав персональных данных, обрабатываемых в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», определен в Перечне персональных данных, подлежащих защите в медицинских информационных системах.

7. Допуск и доступ работников НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» к обработке персональных данных субъектов персональных данных осуществляется в порядке, определенном актуальным Положением о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн (далее - Порядок), утвержденным приказом главного врача.

8. Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением следующих случаев:

1) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом;

2) обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» функций, полномочий и обязанностей, в том числе при перенаправлении обращений граждан, содержащих вопросы, решение которых не входит в компетенцию НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», в соответствующий орган, организацию или должностному лицу по принадлежности в соответствии с Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»;

3) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

4) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации НУЗ «Узловой больницей на ст. Стерлитамак ОАО «РЖД» своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

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

6) обработка персональных данных необходима для осуществления прав и законных интересов НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

8) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

9) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции и об обязательных видах страхования и в соответствии со страховым законодательством;

10) в иных случаях, предусмотренных законодательством Российской Федерации.

9. Субъект персональных данных вправе отозвать согласие на обработку персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных их обработка может быть продолжена без согласия субъекта персональных данных при наличии оснований, указанных в пункте 8 настоящего Положения, и иных оснований, предусмотренных законодательством Российской Федерации.

10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», запись, систематизация, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан Российской Федерации должны осуществляться с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных федеральными законами.

11. Для фиксации персональных данных, цели обработки которых заведомо несовместимы, используются отдельные материальные носители (бумажные или съемные машинные), отдельные базы данных или файлы на несъемных машинных носителях.

12. При обработке различных категорий персональных данных для каждой категории персональных данных используются отдельные материальные носители (бумажные или съемные машинные), отдельные базы данных или файлы на несъемных машинных носителях.

13. Все машинные носители персональных данных, эксплуатируемые в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» учитываются в соответствующих журналах учета. Съемные и несъемные машинные носители персональных данных (внутренние жесткие диски) автоматизированных рабочих мест могут учитываться как в журналах по форме согласно приложению № 1 к настоящего положения. В качестве номеров машинных носителей могут использоваться идентификационные (серийные) номера машинных носителей, присвоенные их производителями, номера инвентарного учета, в том числе инвентарные номера технических средств (системного блока, моноблока и т.п.), имеющих встроенные носители информации (внутренние жесткие диски). Несъемные машинные носители персональных данных, входящие в состав средств вычислительной техники информационных систем, могут учитываться в технических паспортах информационных систем в установленном ОАО «РЖД» порядке. В этом случае в журнале учета несъемных машинных носителей персональных данных учетный номер присваивается всей информационной системе в целом.

14. Сроки обработки (в том числе хранения) персональных данных определяются Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным приказом Минкультуры России от 25 августа 2010 г. № 558, и другими законными актами.

15. Персональные данные подлежат уничтожению в следующих случаях и в указанные сроки:

1) по достижению целей обработки - в 30-дневный срок;

2) в случае утраты необходимости достижения целей обработки - в 30-дневный срок;

3) в случае отзыва субъектом персональных данных согласия на обработку персональных данных - в 30-дневный срок, если иной не предусмотрен федеральными законами, договором или соглашением между НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» и субъектом персональных данных;

4) при выявлении неправомерной обработки персональных данных - в срок, не превышающий 10 рабочих дней с даты выявления.

16. Передача персональных данных субъектов персональных данных без их согласия допускается:

1) третьим лицам с целью предупреждения угрозы жизни и здоровью субъекта персональных данных (например, передача персональных данных в учреждения здравоохранения);

2) в автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже) транспортных средств (АЦБПДП) Министерства транспорта Российской Федерации с целью обеспечения транспортной безопасности;

3) в налоговые органы (например, при направлении НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» налоговой отчетности);

4) по мотивированному запросу органов прокуратуры, правоохранительных органов и органов безопасности, по запросу от государственных инспекторов труда при осуществлении ими надзорно- контрольной деятельности;

5) в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом, по перечню оповещаемых органов и сроков направления извещений о несчастном случае, установленному Трудовым кодексом Российской Федерации.

17. Передача персональных данных в случае, если НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» поручает их обработку третьим лицам, осуществляется в соответствии с заключенными договорами на оказание услуг и с письменного согласия субъектов персональных данных. Договор должен содержать перечень действий (операций) с персональными данными, цели обработки, обязанность лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии с законодательством Российской Федерации и нормативными документами НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД». Перед заключением договора с третьими лицами необходимо запросить у них документы либо их надлежащим образом заверенные копии, подтверждающие выполнение условий соблюдения конфиденциальности и обеспечения безопасности персональных данных субъектов персональных данных при их обработке, в том числе:

1) политика (положение, порядок и др.) оператора по обработке и защите персональных данных;
2) акт определения уровня защищенности персональных данных;

3) модель угроз безопасности персональных данных;

4) документы, описывающие состав и содержание мер по обеспечению безопасности персональных данных, аттестаты соответствия требованиям по безопасности информации для установленного уровня защищенности персональных данных, и другие документы.

18. Обработка персональных данных в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» может осуществляться автоматизированным, неавтоматизированным и смешанным способами. В процессе обработки персональных данных допускается многократный переход от неавтоматизированного способа обработки к автоматизированному и наоборот.

III. Неавтоматизированная обработка персональных данных

19. Уполномоченные работники, осуществляющие неавтоматизированную обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, осуществляемой без использования средств вычислительной техники, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных федеральными законами, нормативными правовыми актами органов исполнительной власти Российской Федерации, а также нормативными документами НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД». Персональные данные при их неавтоматизированной обработке обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

20. Персональные данные фиксируются на материальном носителе неавтоматизированным способом (например, записью «от руки» на листе бумаги) или автоматизированным способом (выводом на печать или копированием информации, содержащей персональные данные, на носитель с использованием средств вычислительной техники).

21. Бумажные носители и съемные машинные носители персональных данных хранятся в сейфах, запираемых шкафах или ящиках столов, находящихся в помещениях НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД». Перечни указанных помещений формируются ответственными за организацию обработки персональных данных и утверждаются главным врачом НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» согласно приложению № 2 к настоящему Положению.

22. Материальные носители, содержащие персональные данные, обрабатываемые в различных целях, хранятся раздельно (в разных шкафах, на разных полках, в отдельных ящиках или папках и т.п.).

23. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, анкеты, карточки, реестры, журналы и др.) должны содержать сведения о цели обработки персональных данных, наименование и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных. Указанные сведения должны отражаться хотя бы в одном из связанных с типовой формой документов (включая саму типовую форму);

2) типовая форма должна исключать объединение полей, предназначенных для персональных данных, цели обработки которых заведомо не совместимы;

3) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных имел возможность ознакомиться со своими персональными данными, не нарушая прав и законных интересов иных субъектов персональных данных;

4) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных.

24. Систематизация обрабатываемых в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» документов, содержащих персональные данные, производится согласно утвержденной в номенклатуре дел. Разработка номенклатуры дел проводится с учетом требований о раздельном хранении персональных данных, цели обработки которых заведомо несовместимы, и сроков хранения, определяемых пунктом 14 настоящего Положения.

25. При ознакомлении субъекта персональных данных со своими персональными данными обеспечивается невозможность его ознакомления с персональными данными иных лиц, содержащимися на тех же бумажных носителях (путем извлечения документов из дела, закрытия чистым листом бумаги и т.п.).

26. При необходимости использования или распространения части персональных данных, находящихся на бумажном носителе, эти персональные данные копируются на другой бумажный носитель.

27. Удаление или обезличивание части персональных данных, если это допускается бумажным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на бумажном носителе (вымарывание).

28. Уточнение персональных данных производится путем обновления или изменения данных на бумажном носителе, а если это не допускается особенностями бумажного носителя - путем фиксации на том же бумажном носителе сведений о вносимых в них изменениях либо путем изготовления нового бумажного носителя с уточненными персональными данными.

29. Бумажные носители, содержащие персональные данные, включая черновики и промежуточные версии рабочих документов, подлежат уничтожению либо содержащиеся в них персональные данные подлежат обезличиванию по достижении целей обработки или в случае утраты необходимости достижения этих целей, а также по окончании срока их хранения.

Особенности неавтоматизированной обработки персональных данных, содержащихся на съемных машинных носителях

30. При необходимости использования или распространения части персональных данных, находящихся на съемном машинном носителе, эти персональные данные копируются на другой съемный машинный носитель, учтенный согласно пункту 13 настоящего Положения.

31. Персональные данные, записанные на съемные машинные носители, удаляются в соответствии с требованиями третьего абзаца пункта 40 настоящего Положения.

32. Съемные машинные носители, не допускающие возможности удаления персональных данных, уничтожаются путем физического разрушения машинного носителя, не позволяющего произвести последующее считывание или восстановление записанных на машинном носителе персональных данных. В журнале учета машинных носителей персональных данных производится соответствующая запись об уничтожении, заверенная подписями уполномоченного работника и лица, осуществляющего учет машинных носителей подразделения.

IV. Автоматизированная обработка персональных данных

33. Автоматизированная обработка персональных данных производится с помощью средств вычислительной техники, как установленных локально, так и объединенных в информационные системы.

34. При автоматизированной обработке персональные данные содержатся на машинных носителях персональных данных. Фиксация персональных данных на машинном носителе производится с использованием средств вычислительной техники (копирование персональных данных на любой съемный или несъемный машинный носитель, ввод персональных данных в базу данных и т.п.).

35. Уточнение персональных данных производится путем обновления или изменения данных на машинном носителе с помощью средств вычислительной техники. Если это не допускается особенностями машинного носителя, то уточнение производится путем изготовления нового машинного носителя с уточненными персональными данными.

36. Обезличивание персональных данных, обрабатываемых в информационных системах НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», в случае необходимости осуществляется с учетом Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, утвержденных приказом Роскомнадзора от 5 сентября 2013 г. № 996.

37. При выявлении по обращению субъекта персональных данных либо Роскомнадзора неточных персональных данных в информационной системе НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» организуется блокирование таких персональных данных на период проверки. В течение 7 рабочих дней со дня подтверждения факта неточности персональные данные уточняются в соответствии с пунктом 35 настоящего положения и разблокируются.

38. При выявлении по обращению субъекта персональных данных либо Роскомнадзора неправомерной обработки персональных данных в информационной системе НУЗ «Узловая больница на ст. Стерлитамак» ОАО «РЖД» организуется блокирование таких персональных данных на период расследования. В течение 3 рабочих дней с момента выявления неправомерной обработки персональных данных такая обработка прекращается. В случае если 15 обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных, такие персональные данные уничтожаются.

39. Об устранении допущенных нарушений или об уничтожении (невозможности уничтожения) персональных данных письменно уведомляется автор обращения (субъект персональных данных либо Роскомнадзор) по форме согласно приложению № 3 к настоящего Положения.

40. Удаление персональных данных в информационных системах НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» производится в соответствии с процедурами, определенными в эксплуатационной документации на информационные системы, обрабатывающие персональные данные. Удаление персональных данных на отдельных средствах вычислительной техники (рабочих местах уполномоченных работников) производится штатными средствами информационных и (или) операционных систем. Удаление части персональных данных на съемном машинном носителе, если это допускает носитель, производится с использованием штатных средств информационных и (или) операционных систем с сохранением возможности обработки иных данных, зафиксированных на машинном носителе.

41. Копирование информации с одного съемного машинного носителя персональных данных на другой и уничтожение персональных данных на съемном машинном носителе производятся только на средствах вычислительной техники, предназначенных для обработки персональных данных.

42. При отправке средств вычислительной техники, предназначенных для обработки персональных данных, для проведения гарантийных и ремонтных работ машинные носители персональных данных из них предварительно удаляются.

43. Если ремонту подлежат машинные носители, содержащие персональные данные, имеющаяся на них информация гарантированно уничтожается. Если гарантированное уничтожение информации на машинных носителях персональных данных невозможно, то такие машинные носители ремонту не подлежат и должны быть физически уничтожены в соответствии с требованиями пункта 44 настоящего Положения.

44. Пришедшие в негодность или отслужившие установленный срок машинные носители персональных данных уничтожаются путем физического разрушения машинного носителя, не позволяющего произвести последующее считывание или восстановление записанных на машинном носителе персональных данных. Уничтожение несъемных машинных носителей персональных данных производится по акту в установленном для средств вычислительной техники порядке. Уничтожение съемных машинных носителей персональных данных может производиться без оформления акта. В журналах учета машинных носителей персональных данных производится соответствующая запись об их уничтожении.

V. Рассмотрение обращений (запросов) субъектов персональных данных

45. Субъекты персональных данных имеют право получать информацию, касающуюся обработки их персональных данных в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», в соответствии с частями 1 – 7 статьи 14 Федерального закона «О персональных данных».

46. При получении обращения (запроса) от субъекта персональных данных ему (или его представителю) предоставляются сведения, касающиеся обработки его персональных данных в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД». Сведения предоставляются в доступной форме, в них не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных. Ответы на письменные запросы граждан и организаций даются в письменной форме.

47. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Федерального закона «О персональных данных» все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ. Запрос должен содержать данные основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения, подтверждающие участие субъекта персональных данных 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 (в том числе электронная) субъекта персональных данных или его представителя.

48. При получении повторного запроса от субъекта персональных данных ранее, чем через 30 дней после первоначального обращения (запроса), и предоставлении ему сведений в полном объеме по результатам рассмотрения первоначального обращения (запроса) НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» вправе отказать субъекту персональных данных в выполнении повторного запроса.

49. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных» в том случае, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

50. Ответы на письменные запросы субъектов персональных данных и организаций даются в письменной форме в объеме, обеспечивающем конфиденциальность персональных данных. Мотивированный отказ в предоставлении запрашиваемой информации направляется, если субъект персональных данных или организация не обладает правами доступа к запрашиваемой информации или запрос не соответствует требованиям Федерального закона "О персональных данных".

51. Учет обращений (запросов) субъектов персональных данных ведется в журнале учета, составленном по форме согласно приложению N 4.

VI. Обеспечение безопасности персональных данных при их обработке

52. Обеспечение безопасности персональных данных при их обработке в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» осуществляется в соответствии:

1) с законодательством Российской Федерации в области обработки и защиты персональных данных;

2) с требованиями ФСТЭК России, ФСБ России и Роскомнадзора;

3) с нормативными документами ОАО «РЖД».

53. Комплекс мер, обеспечивающих безопасность персональных данных, включает в себя в том числе:

1) организацию работы с персональными данными, обеспечивающей сохранность носителей персональных данных и средств защиты информации;

2) размещение информационных систем, обрабатывающих персональные данные, и специального оборудования в помещениях, исключающих возможность неконтролируемого пребывания в них посторонних лиц;

3) разграничение доступа пользователей и работников, обслуживающих средства вычислительной техники, к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

4) учет документов и информационных массивов, содержащих персональные данные;

5) регистрацию действий пользователей информационных систем, обрабатывающих персональные данные, и работников, обслуживающих средства вычислительной техники в установленном НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» порядке;

6) контроль действий и недопущение несанкционированного доступа к персональным данным пользователей информационных систем НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» и персонала, обслуживающего средства вычислительной техники;

7) хранение и использование материальных носителей персональных данных, исключающих их хищение, подмену и уничтожение;

8) необходимое резервирование технических средств и дублирование массивов и носителей информации, содержащей персональные данные.

54. Для каждой информационной системы, обрабатывающей персональные данные, в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119, в зависимости от уровня защищенности персональных данных при их обработке в информационных системах назначается должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе.

55. Организационные и (или) технические меры защиты для каждой информационной системы, обрабатывающей персональные данные, определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД». Уровень защищенности информационных систем, обрабатывающих персональные данные, определяется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

56. Обработка персональных данных осуществляется уполномоченными работниками с обязательным принятием мер, исключающих возможность ознакомления с персональными данными посторонних лиц, в том числе работников НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», не уполномоченных на обработку персональных данных, таких как:

1) экран монитора размещается таким образом, чтобы исключить возможность просмотра информации посторонними лицами (в том числе другими работниками подразделения);

2) уполномоченные работники используют для доступа к информационным системам, обрабатывающим персональные данные, индивидуальные пароли, отвечающие установленным в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» требованиям;

3) средства вычислительной техники блокируются с помощью защищенной паролем экранной заставки во время перерывов в работе;

4) в информационных системах, обрабатывающих персональные данные, и (или) на отдельных автоматизированных рабочих местах, предназначенных для работы с персональными данными, в обязательном порядке используются средства антивирусной защиты. При отсутствии таких средств или окончании срока действия лицензии на них подается соответствующая заявка администратору безопасности;

5) бумажные носители, содержащие персональные данные, размещаются таким образом, чтобы исключить возможность просмотра информации посторонними лицами (в том числе другими работниками подразделения);

6) все бумажные или съемные машинные носители с персональными данными помещаются в сейфы, запираемые шкафы или ящики столов после окончания работы с ними либо при оставлении рабочего помещения;

7) испорченные бланки, черновики и промежуточные редакции документов, содержащие персональные данные, по окончании работы с ними уничтожаются в соответствии с Инструкцией по делопроизводству и документированию управленческой деятельности в НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД».

57. При работе с персональными данными уполномоченным работникам запрещается:

1) работать под чужими или общими учетными записями в информационных системах, обрабатывающих персональные данные, и передавать кому-либо индивидуальные пароли;

2) допускать использование своего автоматизированного рабочего места другими работниками НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» и посторонними лицами;

3) использовать (загружать, запускать и т.п.) для обработки персональных данных программные средства, не разрешенные для применения в информационных системах НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД»;

4) сообщать ставшие им известными в связи с исполнением своих должностных обязанностей персональные данные лицам, не имеющим права доступа к этим данным;

5) делать копии документов, содержащих персональные данные, не требующиеся для выполнения своих служебных обязанностей;

6) держать на рабочем месте материальные носители с персональными данными дольше времени, необходимого на их обработку.

58. Работник НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД» немедленно ставит в известность руководителя своего подразделения:

1) о факте утраты (утери, хищения) материальных носителей персональных данных;

2) о факте разглашения или неправомерной обработки персональных данных;

3) о ставших известными ему фактах или возможностях несанкционированного доступа к информационным системам, обрабатывающим персональные данные.

VII. Правила работы с обезличенными персональными данными

59. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных департамента здравоохранения и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

60. Способы обезличивания при условии дальнейшей обработки персональных данных:

1) уменьшение перечня обрабатываемых сведений;

2) замена части сведений идентификаторами;

3) обобщение – понижение точности некоторых сведений;

4) деление сведений на части и обработка в разных информационных системах;

5) другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных. Для обезличивания персональных данных допустимы любые способы явно не запрещенные законодательно.

61. Решение о необходимости обезличивания персональных данных принимается главным врачом. Сотрудники, ответственные за обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

62. Сотрудники отделов, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

63. Обезличенные персональные данные не подлежат разглашению и могут обрабатываться как с использованием, так и без использования средств автоматизации.

64. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

1) инструкции по организации парольной защиты ;

2) инструкции по антивирусной защите;

3) порядка резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

4) положения о пропускном и внутриобъектовом режиме.

65.При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) правил хранения бумажных носителей;

2) положения о пропускном и внутриобъектовом режиме.

Приложение 1

Журнала учета носителей информации, на которых разрешается хранение персональных данных

№ п/п	Регистрационный номер	Тип/ёмкость машинного носителя персональных данных	Место установки (использования)	Ответственное должностное лицо (ФИО)	Расписка в получении (подпись, дата)	Расписка в обратном приеме (подпись, дата)	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)

Приложение 2

«УТВЕРЖДАЮ»
Главный врач
НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД»
_____ Ю.В. Саидгалина
«_____» _____20__ г.

Перечень помещений НУЗ «Узловая больница на ст. Стерлитамак ОАО «РЖД», в которых хранятся материальные носители персональных данных

№	Номер помещения	Адрес (место расположения)

Приложение 3

УВЕДОМЛЕНИЕ

об устранении нарушений обработки или уничтожении (невозможности уничтожения) персональных данных

Уважаемый(ая) _____!

(ФИО)

Настоящим уведомляем, что Ваше обращение от _____

(дата обращения,

_____

краткое содержание обращения)

_____рассмотрено.

Выявленное(ые) нарушение(я) обработки Ваших персональных данных:

_____

(краткое описание нарушения)

_____

(устранены, уничтожены/уничтожение невозможно по причине)

_____/_____/_____

(должность) (подпись) (расшифровка подписи)

«____»_____20___г.

Приложение 4

Журнала учета обращений (запросов) субъектов персональных данных

№ п/п	Дата поступления обращения (запроса) в подразделение	Ф.И.О. заявителя	Адрес места жительства заявителя	Количество листов обращения (запроса)	Дата, входящий номер, откуда поступило обращение (запрос), форма обращения (личное, письменное, электронное, почтовое)	Краткое содержание	Исполнитель ответа на обращение (запрос) (должность, фамилия)	Исходящий номер и дата ответа, номер и дата почтового отправления