РЖД МЕДИЦИНА

Частное учреждение здравоохранения «Больница «РЖД-МЕДИЦИНА» города Волхов»

«УТВЕРЖДАЮ»

Главный врач

Р.В.Марковиченко

21.06.2021 года

ПОРЯДОК
обработки и обеспечение защиты режима персональных данных работников частного учреждения здравоохранения « Больница «РЖД-Медицина» города Волхов»

I. Общие положения

1. Настоящий Порядок, разработанный в соответствии с законодательством Российской Федерации в области обработки и защиты персональных данных, политикой частного учреждения здравоохранения « Больница «РЖД-Медицина» города Волхов» (далее - Учреждение) по обработке и защите персональных данных, Политикой по обработке и защите персональных данных работников Учреждения и другими нормативными документами Учреждения, устанавливает единые корпоративные требования к обработке и обеспечению режима защиты персональных данных работников Учреждения.

2. Требования настоящего Порядка обязательны для выполнения работниками структурных подразделений Учреждения (далее подразделений).

3. В настоящем Порядке используются следующие понятия и термины:

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

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

3) разглашение персональных данных - действия (бездействие), в результате которых персональные данные в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без письменного согласия субъекта персональных данных;

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

5) удаление персональных данных-действия, в результате которых становится невозможным ознакомиться с их содержанием в информационной системе персональных данных;
6) вымарывание персональных данных -действия, исключающие дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе;
7) уполномоченный орган по защите прав субъектов персональных данных - федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);
8) контролируемая зона-пространство (административные здания Учреждения, прилегающая к ним территория), на котором на законных основаниях осуществляется контроль за пребыванием и действиями физических лиц и (или) транспортных средств;
9) материальный носитель - бумажный или машинный носитель, 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) электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах Учреждения;
12) ПЭВМ- персональная электронная вычислительная машина;
13) СНИ-съемные машинные носители информации, используемые для хранения информации вне ПЭВМ (флэш-накопители, внешние жесткие диски, CD-диски и иные устройства).

Понятия «работник», «персональные данные», «субъекты персональных данных», «подразделения Учреждения», «ответственный за организацию обработки персональных данных в подразделении», «уполномоченные работники», «информационная система Учреждения», «обработка персональных данных», «автоматизированная обработка персональных данных», «неавтоматизированная обработка персональных данных», «передача персональных данных», «распространение персональных данных», «блокирование персональных данных», «уничтожение персональных данных», «трансграничная передача персональных данных», «конфиденциальность персональных данных», «безопасность персональных данных», «защита персональных данных», «режим защиты персональных данных» используются в настоящем Порядке в значениях, которые предусмотрены в пункте 6 Политики по обработке и защите персональных данных Учреждения.

II. Допуск и доступ к обработке персональных данных

1.Основанием для допуска работника к обработке персональных данных является приказ о назначении его на должность, должностная инструкция, предусматривающая обработку персональных данных, обязательство о неразглашении персональных данных, составленное по форме согласно приложению № 1.

2.Руководитель подразделения Учреждения:

-назначает приказом, составленным по форме согласно приложению № 2, ответственного за организацию обработки персональных данных;

-утверждает список работников, уполномоченных на обработку персональных данных, составленный по форме согласно приложению №3. Уполномоченные работники имеют право обрабатывать только те персональные данные, которые необходимы для выполнения конкретных функций в определенных целях;

-до предоставления доступа к обработке персональных данных ответственного за организацию обработки персональных данных в подразделении и уполномоченных работников обеспечивает:

а) их ознакомление под подпись с настоящим Порядком;

б) подписание ими обязательства о неразглашении персональных данных, составленного по форме согласно приложению № 1. Обязательство о неразглашении персональных данных хранится в личном деле работника.

3.Обязанности ответственных за организацию обработки персональных данных, а также уполномоченных работников в подразделении включаются в их должностные инструкции.

4.Доступ уполномоченных работников к обработке персональных данных в информационных системах Учреждения осуществляется в соответствии с Порядком предоставления доступа к информационным системам ОАО «РЖД», утвержденным распоряжением ОАО «РЖД» от 28 ноября 2011 г.№ 2546р.

5.Представители сторонних организаций допускаются к обработке персональных данных на основании заключаемых договоров в соответствии с требованиями, изложенными в пункте 21 настоящего Порядка.

III. Требования к обработке персональных данных

1.Требования к обработке персональных данных, устанавливаемые настоящим Порядком, распространяются на персональные данные, состав и категории которых, а также перечень документов, их содержащих, определены в разделе III Положения об обработке и защите персональных данных работников Учреждения».

Обработка персональных данных, не отвечающая целям обработки, запрещается.

2.При приеме на работу уполномоченный работник получает у субъекта персональных данных согласие на обработку его персональных данных, в том числе на включение персональных данных в общедоступные источники персональных данных (корпоративные справочники, адресные книги), которое оформляется по форме согласно приложению №4.

3.В случаях, предусмотренных Федеральными законами, когда обработка

персональных данных субъекта персональных данных осуществляется только с его согласия, уполномоченный работник получает у субъекта персональных данных согласие на обработку его персональных данных, составленное по форме согласно приложению №5.

4.Согласие на обработку персональных данных уполномоченный работник получает у субъекта персональных данных до начала их обработки.
5.Согласия на обработку персональных данных работников хранятся в их личных делах.
6.Получение согласия близких родственников работника на обработку их персональных данных не требуется при заполнении анкет в объеме, предусмотренном унифицированной формой N№Т-2, либо в случаях, установленных законодательством Российской Федерации (исполнение законодательства в сфере транспортной безопасности, получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат и другие случаи).
7.В иных случаях получение согласия близких родственников работника является обязательным условием обработки их персональных данных и оформляется по форме согласно приложению №5.
8.Субъект персональных данных вправе отозвать согласие на обработку персональных данных, направив в Учреждение отзыв, составленный по форме согласно приложению №6, либо в произвольной форме.
9.В случае отзыва субъектом персональных данных согласия на обработку персональных данных Учреждения вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных законодательством Российской Федерации.
10.Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее по форме согласно приложению №7, и дать письменное согласие на получение персональных данных у третьих лиц, составленное по форме согласно приложению №8.

Учреждение сообщает работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника от дачи письменного согласия на их получение.

Необходимость согласия на получение персональных данных у третьих лиц и направления уведомления об этом может возникнуть, например, при подтверждении факта получения диплома, свидетельства, аттестата об образовании, при восстановлении трудовой книжки, свидетельства о получении квалификации, при подтверждении факта работы в том или ином месте, факта смены фамилии и др., в том числе если утрата сведений произошла в связи со стихийными бедствиями, иными обстоятельствами.
11.Учреждение не вправе запрашивать у третьих лиц даже с согласия субъекта персональных данных информацию, не имеющую отношения к целям обработки персональных данных.
12. Учреждение вправе поручить обработку персональных данных субъектов персональных данных с их согласия другому лицу на основании заключаемого с ним договора.

13. 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, настоящим Порядком и иными нормативными документам и У чреждения.

14. Если при обращении субъекта персональных данных либо уполномоченного органа по защите прав субъектов персональных данных выявлены неточные персональные данные или неправомерная обработка персональных данных, Учреждение обязано осуществить блокирование таких персональных данных с момента обращения на период проверки.

При подтверждении факта неточности персональных данных Учреждение обязано уточнить персональные данные в течение 7 рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

При выявлении неправомерной обработки персональных данных Учреждение обязано прекратить их обработку в срок, не превышающий 3 рабочих дней с даты выявления. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение обязано уничтожить такие персональные данные в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных.

Об устранении допущенных нарушений или об уничтожении (невозможности уничтожить) персональных данных Учреждение обязано письменно уведомить субъекта персональных данных по форме согласно приложению №9 или устно и приобщить копию уведомления или справку об уведомлении к материалам расследования (проверки).

В случае если обращение субъекта персональных данных, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, Учреждение обязано уведомить указанный орган.

15. Обработка персональных данных кандидатов для приема на работуосуществляется в соответствии с требованиями раздела III настоящего Порядка. При обработке персональных данных кандидатов оформляется согласие по форме согласно приложению №5.

При этом для кандидатов, поступающих на работу, действует несколько особых случаев:

1) письменное согласие не требуется, если от имени кандидата действует кадровое агентство, с которым данное лицо заключило соответствующий договор, а также при самостоятельном размещении кандидатом своего резюме в сети Интернет, доступного неограниченному кругу лиц;
2) письменное согласие кандидата не требуется при поступлении резюме кандидата из банка вакансий, размещенных на сайте Учреждения, так как согласие заполняется при размещении резюме на сайте;
3) если резюме кандидата поступило по электронной почте или факсу, уполномоченному работнику необходимо подтвердить факт направления указанного резюме самим кандидатом. Если из резюме невозможно однозначно определить физическое лицо, его направившее, данное резюме подлежит уничтожению в день поступления.

16.Обезличивание персональных данных, обрабатываемых в информационных системах Учреждения, в случае необходимости осуществляется с учетом Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утвержденных приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. №996

Обязанности лиц, осуществляющих проведение мероприятий по обезличиванию персональных данных, включаются в их должностные инструкции.

17.Сроки хранения, комплектования, учета, передачи и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов регламентируются Федеральным законом «Об архивном деле в Российской Федерации», 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, Перечнем документов, образующихся в деятельности ОАО «РЖД», с указанием сроков хранения, утвержденным распоряжением ОАО «РЖД» от 28 декабря 2007 г. No 2474р, Инструкцией по делопроизводству и документированию управленческой деятельности в ОАО «РЖД», утвержденной приказом ОАО «РЖД» от 17 июня 2013 г. №5 5,Инструкцией по кадровому делопроизводству ,утвержденной распоряжением ОАО «РЖД» от 30 июня 2006 г. № 1335р.

18.Безопасность персональных данных обеспечивается реализацией комплекса мер, определенных Федеральными Законами, указами Президента Российской Федерации, постановлениями Правительства Российской Федерации, приказами ФСТЭК России, ФСБ России, Роскомнадзора, нормативными документами Учреждения, в том числе включающих:

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

2) размещение информационных систем Учреждения 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, информационных массивов, содержащих персональные данные;

5)регистрацию действий пользователей информационных систем и работников, обслуживающих средства вычислительной техники, в порядке, принятом Учреждением»;

6)контроль действий и недопущение несанкционированного доступа к персональным данным пользователей информационных систем Учреждения персонала, обслуживающего средства вычислительной техники;

7)хранение и использование материальных носителей, исключающих их

хищение, подмену и уничтожение;

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

Для каждой информационной системы Учреждения организационные и (или) технические меры определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе.

19.Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

20.При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

21.При использовании типовых форм документов, в которые предполагается или допускается включение персональных данных, должны соблюдаться условия, предусмотренные пунктом 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в контролируемую зону или в иных аналогичных целях, должны соблюдаться условия, предусмотренные пунктом 8 указанного положения.

22.Уточнение персональных данных производится путем их обновления или изменения на материальном носителе, а если это не допускается особенностями материального носителя -путем изготовления нового материального носителя с уточненными персональными данными.

23.При работе с документами, содержащими персональные данные, должны быть приняты меры, исключающие возможность ознакомления с этими документами посторонних лиц, в том числе работников, не уполномоченных на обработку персональных данных.

24.Документы, содержащие персональные данные, должны храниться в специальном шкафу или помещении, обеспечивающем защиту от несанкционированного доступа.
25. Дела, содержащие персональные данные, должны находиться в рабочих кабинетах или в специально отведенных для их хранения помещениях, располагаться в запираемых шкафах, обеспечивающих их полную сохранность.
26. Средства защиты информации, обеспечивающие защиту персональных данных, должны удовлетворять требованиям, утвержденным 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», а также нормативным правовым актам в области обработки и защиты персональных данных Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.
27. Автоматизированная обработка персональных данных разрешается только при условии применения средств защиты информации, обеспечивающих нейтрализацию актуальных угроз, определенных частью 5 статьи 19 Федерального закона «О персональных данных».
28. Во время эксплуатации средств вычислительной техники, предназначенных для обработки персональных данных, должны быть предусмотрены меры по исключению случаев несанкционированного подключения к внешним информационным системам, внешним информационно - телекоммуникационным сетям, а также несанкционированного доступа к этим средствам при проведении ремонтных, профилактических и других видов работ.
29.Обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
30.Во время перерывов в работе, а также после окончания работы с документами, содержащими персональные данные, необходимо:

- убирать документы с поверхности рабочих столов в запирающееся хранилище (сейф, шкаф);
- блокировать средство вычислительной техники с помощью защищенной паролем экранной заставки;
- принимать необходимые меры по недопущению использования средства вычислительной техники другими работниками и посторонними лицами.

IV. Требования к обращению с материальными носителями персональных данных, их учет и хранение

1.Требования к подготовке, оформлению, обработке, прохождению (согласованию), регистрации и хранению бумажных носителей персональных данных определяются нормативными документами Учреждения устанавливающими порядок ведения делопроизводства, с учетом положений, предусмотренных настоящим Порядком.
2.Персональные данные субъектов персональных данных хранятся на бумажных носителях в соответствии с номенклатурой дел и в электронном виде (в

информационных системах Учреждения на ПЭВМ, а также на съемных магнитных, оптических и других цифровых носителях), с соблюдением условий, обеспечивающих их защиту от несанкционированного доступа.

3.Черновики и рабочие варианты документов, содержащих персональные данные, уничтожаются исполнителем без возможности восстановления.

4.При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

Хранение материальных носителей должно осуществляться в помещениях, находящихся в контролируемой зоне.

5.Руководителем подразделения Учреждения утверждается перечень помещений, в которых хранятся материальные носители персональных данных, по форме согласно приложению №10.

6.Копирование и печатание документов, содержащих персональные данные, должно осуществляться в порядке, исключающем возможность нарушения конфиденциальности персональных данных.

7.При изъятии из дел или перемещении из одного дела в другое документов, содержащих персональные данные, производится соответствующая отметка во внутренней описи дела, в которой указывается новое местонахождение документа.

При необходимости вместо изъятых документов в дело могут быть подшиты их заверенные копии.

8.Машинные носители учитываются в журнале учета машинных носителей персональных данных, составленном по форме согласно приложению №11.

9.Все находящиеся на хранен ии ив обращении СНИ с персональными данными подлежат учету. Каждый СНИ, предназначенный для работы с персональными данными, должен иметь этикетку, на которой указывается его регистрационный номер, условное или сокращенное название подразделения.

10.Запрещается:

- хранить СНИ, содержащие персональные данные, на рабочих местах ненадлежащим образом или передавать на хранение другим лицам;
- выносить СНИ, содержащие персональные данные, из рабочих помещений без служебной необходимости.

V. Уничтожение персональных данных и их материальных носителей

1.Подразделения Учрежения осуществляют систематический мониторинг персональных данных, цели обработки которых достигнуты или сроки хранения которых истекли, с последующим уничтожением документов, иных материальных носителей, содержащих персональные данные, а также удалением персональных данных, содержащихся в информационных системах Учреждения файлах, хранящихся на ПЭВМ или на внешних перезаписываемых СНИ, в соответствии с законодательством Российской Федерации или при наступлении иных законных оснований.

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

1) по достижении целей обработки персональных данных -в 30-дневный срок;
2) в случае утраты необходимости в достижении целей обработки персональных

данных -в 30-дневный срок;
3) в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных -в 30-дневный срок, если иной срок не предусмотрен договором или соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами;
4) при выявлении неправомерной обработки персональных данных -в срок, не превышающий 10 рабочих дней с даты выявления, в следующих случаях:
а) персональные данные являются неполными, устаревшими, неточными (при условии, что уточнение персональных данных невозможно);
б) персональные данные получены незаконно;
в) персональные данные не являются необходимыми для заявленной цели обработки.
3.Отбор к уничтожению дел (документов), содержащих персональные данные, и их уничтожение проводятся на основании документов, указанных в пункте 25 настоящего Порядка.
В процессе уничтожения дел и документов необходимо исключить возможность ознакомления посторонних лиц с содержащимися в них персональными данными.
4.Уничтожение не вошедших в дела документов (копий документов), содержащих персональные данные, должно производиться в подразделении Учреждения путем сжигания или с помощью бумагорезательной машины. При этом должна быть исключена возможность прочтения текста уничтоженного документа. В учетных формах регистрации документа при необходимости производится соответствующая запись об уничтожении, заверенная подписями исполнителя и работника подразделения, который осуществляет регистрацию документов.
5.Уничтожение персональных данных, хранящихся в информационных системах, производится в соответствии с порядком:, установленным в Учреждении.
6.Уничтожение персональных данных, хранящихся на ПЭВМ и (или) на перезаписываемых СНИ, производится с использованием штатных средств информационных и операционных систем.
7.Уничтожение СНИ производится путем механического нарушения целостности СНИ, не позволяющего произвести считывание или восстановление содержания персональных данных (надлом, физическое деформирование). В журнале учета машинных носителей персональных данных производится соответствующая запись об уничтожении, заверенная подписями исполнителя и уполномоченного работника подразделения Учреждении, который осуществляет регистрацию СНИ.
8.Уничтожение или обезличивание части персональных данных, если это допускает материальный носитель, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
9.При утрате или несанкционированном уничтожении СНИ проводится служебное расследование и составляется акт. Соответствующие отметки производятся в журнале учета машинных носителей персональных данных.

VI. Передача персональных данных

1.Передача персональных данных субъектов персональных данных без их согласия допускается, если это необходимо для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве, по мотивированным запросам правоохранительных органов и иных органов государственной власти в рамках установленных полномочий, а также в иных случаях предусмотренных федеральными законами.

2.Передача персональных данных субъектов персональных данных третьим лицам осуществляется с их письменного согласия, составленного по форме согласно приложению №12, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъектов персональных данных, а также в иных случаях, предусмотренных Федеральным законом «О персональных данных», Трудовым кодексом Российской Федерации и иными федеральными законами.

Передача персональных данных третьим лицам осуществляется только после получения от третьего лица заверенных в установленном порядке документов, подтверждающих выполнение условий соблюдения конфиденциальности и обеспечения безопасности персональных данных при их обработке.

3.Передача персональных данных субъектов персональных данных общественным организациям, негосударственным пенсионным фондам и страховым компаниям осуществляется в соответствии с заключенными с этими организациями договорами на оказание услуг и с письменного согласия субъектов персональных данных, составленного по форме согласно приложению №4.

При этом в текст договора включаются условия соблюдения конфиденциальности и обеспечения безопасности персональных данных, обрабатываемых в рамках выполнения обязательств по договору согласно требованиям Федерального закона «О персональных данных», Положения об обработке и защите персональных данных работников Учреждения и настоящего Порядка.

4.Пересылка материальных носителей организациям, государственным органам, а также между подразделениями Учреждения расположенными по различным почтовым адресам, производится в запечатанных конвертах (пакетах) с сопроводительным документом, в котором указывается о наличии персональных данных и требование о соблюдении конфиденциальности персональных данных.

5.Пересылка конвертов (пакетов) с документами, содержащими персональные данные, может производиться фельдъегерской связью, заказными или ценными почтовыми отправлениями. Допускается передача документов, содержащих персональные данные, нарочным (работником подразделения Учреждения или работником организации - адресата) с распиской о получении документов в реестре.

6.Передача материальных носителей между подразделениями Учреждения осуществляется уполномоченными работниками в соответствии с запросом или письменным поручением руководителя подразделения Учреждения.

Передача дел и СНИ, содержащих персональные данные, осуществляется с распиской о получении в реестре или других учетных формах подразделения.
7.Передача персональных данных при их обработке в информационных системах Учреждения осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных и технических мер, обеспечивающих нейтрализацию актуальных угроз безопасности согласно части 5 статьи 19 Федерального закона «О персональных данных».
8.Запрещается передача персональных данных субъектов персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны и через сеть международного информационного обмена (сети связи общего пользования, Интернет) без применения соответствующих организационных и технических мер защиты.
9.Передача персональных данных, включенных в общедоступные источники персональных данных (фамилия, имя, отчество; место работы; занимаемая должность; номера рабочих телефонов; адреса корпоративной электронной почты) между подразделениями Учреждения может осуществляться по корпоративным каналам связи.
10.При необходимости регистрации в Единой автоматизированной системе документооборота Учреждения документа, содержащего персональные данные, создается и регистрируется карточка сопроводительного документа (входящего, исходящего, организационно-распорядительного) или поручения в соответствии с требованиями Инструкции по делопроизводству и документированию управленческой деятельности в Учреждении. При этом файлы документов, содержащих персональные данные, к карточке не прикрепляются.
11.Пересылка материальных носителей, непосредственная их передача сторонним адресатам осуществляется только с письменного указания руководителя подразделения Учреждения, осуществляющего отправку документа.
12.Трансграничная передача персональных данных субъектов персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, перечень которых утвержден уполномоченным органом по защите прав субъектов персональных данных, осуществляется в соответствии с Федеральным законом- «О персональных данных» и нормативными документами Учреждения.
13.Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:
1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных, составленного по форме согласно приложению № 13;
2) предусмотренных международными договорами Российской Федерации;
3) иреду смотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов

незаконного вмешательства;
4) исполнения договора, стороной которого является субъект персональных данных;
5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.
14.Трансграничная передача персональных данных субъектов персональных данных может быть запрещена или ограничена в целях защиты законных интересов Учреждения и прав субъектов персональных данных.
15.Передача персональных данных через сеть международного информационного обмена (сети связи общего пользования, Интернет) должна осуществляться с использованием сертифицированных средств криптографической защиты информации и в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации.

VII. Рассмотрение обращений (запросов) субъектов персональных данных

1.Субъекты персональных данных имеют право получать информацию, касающуюся обработки их персональных данных в Учреждении в соответствии с частями 1-7 статьи 14 Федерального закона «О персональных данных».
2.Сведения предоставляются субъекту персональных данных 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.
3.Сведения предоставляются субъекту персональных данных или его представителю подразделением Учреждения, осуществляющим обработку персональных данных, при обращении либо при получении запроса.
4.Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждения, подпись субъекта персональных данных или его представителя.

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

В случае если в обращении (запросе) субъекта персональных данных не отражены указанные сведения, то ему направляется мотивированный отказ.
5.В случае если запрашиваемые сведения были предоставлены для ознакомления субъекту персональных данных по его запросу, он вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения этих сведений и ознакомления с ними не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса.

До истечения этого срока субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос 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 пункте 76 настоящего Порядка, должен содержать обоснование направления повторного запроса.

6.Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктом 7 настоящего Порядка. Такой отказ должен быть мотивированным.

7.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.

8.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».

9.Учет обращений (запросов) субъектов персональных данных ведется в журнале учета, составленном по форме согласно приложению №14.

VIII. Проведение служебного расследования по фактам утраты материальных носителей персональных данных, разглашения либо неправомерной обработки персональных данных субъектов персональных данных

1.В случае выявления утраты материальных носителей, разглашения или неправомерной обработки персональных данных в подразделении Учреждения должны быть осуществлены действия, направленные на обеспечение законных прав и свобод субъектов персональных данных, а также приняты исчерпывающие меры по локализации условий, способствовавших нарушению режима защиты персональных, данных, и минимизации ущерба.

2.О фактах утраты материальных носителей, разглашения персональных данных либо неправомерной обработки персональных данных информируется письменно руководитель и ответственный за организацию обработки персональных данных подразделения Учреждения в котором допущено нарушение. Факт нарушения порядка обработки персональных данных фиксируется в журнале учета нарушений порядка обработки персональных данных, составленном по форме согласно приложению №15.

3.Для расследования обстоятельств утраты материальных носителей, разглашения либо неправомерной обработки персональных данных приказом руководителя подразделения Учреждения назначается комиссия по расследованию нарушений обработки персональных данных (далее -комиссия), в состав которой включается ответственный за организацию обработки персональных данных в подразделении. При необходимости в состав комиссии могут быть включены представители иных подразделений Учреждения.

4.При проведении служебного расследования обстоятельств утраты материальных носителей, разглашения либо неправомерной обработки персональных данных

комиссия выполняет следующие функции:
1) определяет обоснованность отнесения разглашенной либо утраченной информации к персональным данным;
2) устанавливает обстоятельства утраты материальных носителей, разглашения либо неправомерной обработки персональных данных (время, место, способ);
3) устанавливает лиц, которые допустили утрату материальных носителей, разглашение либо неправомерную обработку персональных данных;
4)принимает меры к определению местонахождения материальных носителей;
5)устанавливает причины и условия, которые привели к утрате материальных носителей, разглашению либо неправомерной обработке персональных данных;
6)оценивает причиненный или возможный вред субъекту персональных данных вследствие утраты материальных носителей, разглашения либо неправомерной обработки персональных данных;
7)составляет заключение о результата проведенного служебного расследования.
5.Служебное расследование проводится в возможно короткие сроки (не более 20 календарных дней) со дня установления факта утраты материальных носителей, разглашения либо неправомерной обработки персональных данных.
6.Члены комиссии, проводящие служебное расследование, имеют право:
1) опрашивать работников подразделений Учреждения которые допустили утрату материальных носителей, разглашение либо неправомерную обработку персональных данных, а также работников подразделений Учреждении, которые могут оказать содействие в установлении обстоятельств допущенного нарушения или в определении местонахождения утраченных материальных носителей, и получать от них письменные объяснения;
2) запрашивать и получать информацию и документы, имеющие отношение к проведению служебного расследования обстоятельств утраты материальных носителей, разглашения либо неправомерной обработки персональных данных;
3) проводить осмотр помещений, в которых хранятся и обрабатываются персональные данные, рабочих мест уполномоченных работников, обследование средств вычислительной техники, используемых для обработки персональных данных, мест, где могут находиться утраченные материальные носители;
4) проверять количество материальных носителей, учетную документацию, отражающую их поступление и движение;
5) привлекать с разрешения главного врача подразделения Учреждения назначившего служебное расследование, к работе комиссии работников (экспертов), обладающих специальными знаниями.
7.Заключение о результатах проведенного служебного расследования должно содержать следующие сведения:
1) дата и место проведения служебного расследования;
2) состав комиссии, проводившей служебное расследование;
3) основания для проведения служебного расследования;
4) установленные факты о времени, месте и обстоятельствах нарушения;
5) правильность отнесения разглашенной либо утраченной информации к персональным данным;
6) о виновных лицах и степени их вины;
7) наличие умысла в действиях виновных лиц;
8) выводы по результатам определения материального или иного вреда,

причиненного субъекту персональных данных вследствие утраты материальных носителей, разглашения либо неправомерной обработки персональных данных;

9) предложения о прекращении поиска материального носителя и списании его в учетных формах;

10) другие сведения , имеющие отношение к с.тужсебному расследованию;

11) выводы о причинах и условиях совершения нарушений, рекомендации по их устранению.

8.Заключение о проведении служебного расследования должно быть подписано всеми членами комиссии. При несогласии с выводами или содержанием отдельных положений член комиссии подписывает заключение и приобщает к нему свое особое мнение (в письменном виде).

9.По окончании служебного расследования комиссия обязана представить на рассмотрение руководителя подразделения Учреждения назначившего служебное расследование, следующие документы:

1) заключение о результатах проведенного служебного расследования;

2) письменные объяснения работников, которых опрашивали члены комиссии (при необходимости);

3) другие документы, имеющие отношение к служебному расследованию.

10.По окончании служебного расследования руководитель подразделения Учреждения, назначивший служебное расследование, в установленном законодательством Российской Федерации и нормативными документами Учреждения порядке должен принять решение:

1) о привлечении виновных работников к дисциплинарной и (или) материальной ответственности;

2) об обращении в правоохранительные органы с заявлением о привлечении работников, допустивших утрату материальных носителей, разглашение либо неправомерную обработку персональных данных, к административной или уголовной ответственности;

3) о принятии мер по устранению причин и условий, способствовавших нарушению режима защиты персональных данных.

11.Копии заключений по результатам служебного расследования, а также информация о мерах, принятых к работникам, допустившим утрату материальных носителей, разглашение либо неправомерную обработку персональных данных, направляются Учреждении.

IX. Обязанности ответственных за организацию обработки и уполномоченных работников на обработку персональных данных

1.Ответственные за организацию обработки персональных данных и уполномоченные работники обязаны руководствоваться в своей деятельности законодательством Российской Федерации в области обработки и защиты персональных данных, политикой Учреждения по обработке и защите персональных данных, Положением об обработке и защите персональных данных работников Учреждения, настоящим Порядком и другими нормативными документами Учреждения

2.Ответственные за организацию обработки персональных данных в

подразделениях Учреждения обеспечивают:

1) соблюдение законодательства Российской Федерации и нормативных документов Учреждения в области обработки и защиты персональных данных;

2) доведение до сведения уполномоченных работников подразделения Учреждения положений законодательства Российской Федерации и нормативных документов Учреждения в области обработки и защиты персональных данных;

3) осуществление внутреннего контроля за обеспечением режима защиты персональных данных в подразделении Учреждения.

3.Уполномоченные работники обязаны:

1) знать и выполнять законодательные и иные нормативные правовые акты Российской Федерации, а также нормативные документы Учреждения в области обработки и защиты персональных данных;
2) выполнять все требования настоящего Порядка, Положения об обработке и защите персональных данных работников Учреждения и других нормативных документов Учреждения устанавливающих режим защиты персональных данных в Учреждении;
3) не разглашать информацию, содержащую персональные данные субъектов персональных данных;
4) обеспечивать конфиденциальность персональных данных, использовать предусмотренные в Учреждении меры для защиты персональных данных от неправомерных действий;
5) во время работы с информацией и (или) документами, содержащими персональные данные, исключать возможность ознакомления с ними работников, не имеющих права обработки персональных данных;
6) при увольнении сдавать все имеющиеся в распоряжении материальные носители лицу, ответственному за организацию обработки персональных данных в подразделении Учреждения.
7) информировать руководителя подразделения Учреждения обо всех фактах и попытках несанкционированного доступа к персональным данным, и о других нарушениях порядка обработки персональных данных.