

Положение об обработке персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) Государственного бюджетного учреждения здравоохранения «Областная стоматологическая поликлиника» (далее – Учреждение) разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Гражданским кодексом Российской Федерации от 30.11.1994 №51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цель разработки Положения — определение порядка обработки персональных данных граждан, обратившихся в Учреждение и иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Учреждения; обеспечение защиты прав и свобод человека и гражданина, в т.ч. граждан, обратившихся в Учреждение при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом Российской Федерации.

2. Термины и определения

2.1. В настоящем документе используются следующие термины и их определения.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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, уничтожение персональных данных.

Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Субъект персональных данных – физическое лицо, которое может быть однозначно идентифицировано по персональным данным.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

3. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Состав персональных данных, обрабатываемых в ИСПДн Учреждения, определяется «Перечнем персональных данных...».

3.2. Перечень персональных данных утверждается Главным врачом Учреждения.

3.3. Главный врач Учреждения определяет перечень лиц из числа работников, уполномоченных на обработку персональных данных субъектов, обеспечивающих обработку персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", других нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

3.4. Документы со сведениями, содержащими персональные данные, обрабатываются на рабочих местах работников, перечень которых определяется Главным врачом Учреждения.

3.5. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника Учреждения при его приеме, переводе и увольнении.

3.5.1. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

3.5.1.1. паспорт или иной документ, удостоверяющий личность;

3.5.1.2. трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

3.5.1.3. страховое свидетельство государственного пенсионного страхования;

3.5.1.4. документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

3.5.1.5. документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

3.5.1.6. свидетельство о присвоении ИНН (при его наличии у работника).

3.5.2. При оформлении работника в Учреждение заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

3.5.2.1. общие сведения (идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, пол, Ф.И.О. дата рождения, место рождения, гражданство, знание иностранного языка, образование, профессия, стаж работы, состояние в браке, состав семьи, серия, номер и дата выдачи паспорта, наименование органа, выдавшего паспорт, адрес и дата регистрации по месту жительства (месту пребывания), номер телефона);

3.5.2.2. сведения о воинском учете;

3.5.2.3. данные о приеме на работу;

3.5.3. В дальнейшем в личную карточку вносятся:

3.5.3.1. сведения о переводах на другую работу;

3.5.3.2. сведения об аттестации;

3.5.3.3. сведения о повышении квалификации;

3.5.3.4. сведения о профессиональной переподготовке;

3.5.3.5. сведения о наградах (поощрениях), почетных званиях;

3.5.3.6. сведения об отпусках;

3.5.3.7. сведения о социальных льготах.

3.5.4. У Учреждения создаются и хранятся следующие группы документов, содержащие персональные данные работников в единичном или сводном виде:

3.5.4.1. документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений; копии

отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

3.5.4.2. документация по Учреждению, работе отделов (положения, должностные инструкции работников, приказы);

3.5.4.3. документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

3.6. Комплекс документов, сопровождающий процесс работы с гражданами.

3.6.1. Информация, представляемая гражданами либо их представителями в структурные подразделения Учреждения, должна иметь документальную форму. Граждане, либо их представители предъявляют следующие документы:

3.6.1.1. паспорт или иной документ, удостоверяющий личность;

3.6.1.2. полис обязательного медицинского страхования;

3.6.1.3. ИНН;

3.6.1.4. СНИЛС.

3.6.2. При первичном обращении физического лица в Учреждение, работник заполняет установленную форму, в которой отражаются следующие анкетные и биографические данные:

3.6.2.1. фамилия, имя, отчество;

3.6.2.2. пол;

3.6.2.3. дата рождения;

3.6.2.4. гражданство;

3.6.2.5. адрес прописки и дата регистрации;

3.6.2.6. адрес места жительства;

3.6.2.7. сведения о постановленном диагнозе;

3.6.2.8. СНИЛС.

3.6.3. Данные из документов вносятся работниками в электронном виде в ИСПДн. В бумажном виде впоследствии создаются, хранятся и передаются следующие группы документов, содержащие персональные данные граждан, обратившихся в Учреждение, в единичном или сводном виде:

3.6.3.1. карточка пациента;

3.6.3.2. справки по месту требования в соответствии с законом.

4. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Допуск к персональным данным субъекта могут иметь только те работники Учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких работников отражен в «Списке лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей».

4.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

4.2.1. ознакомление работника под роспись с настоящим Положением, «Перечнем персональных данных...» и другими локальными нормативно-правовыми актами Учреждения, касающимися обработки персональных данных;

4.2.2. истребование с работника «Обязательства о неразглашении информации ограниченного доступа»;

4.2.3. внесение работника в «Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей» и в «Журнал учета лиц, допущенных к работе с персональными данными в информационных системах».

4.3. Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения трудовых обязанностей.

4.4. Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

4.5. Любой субъект имеет право, за исключением случаев, предусмотренных законодательством:

4.5.1. на получение сведений об Учреждении в соответствии со ст.14 ФЗ №152 от 27.06.2006 г.;

4.5.2. на ознакомление со своими персональными данными;

4.5.3. на уточнение, блокирование или уничтожение своих персональных данных в случае, если они являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленных Учреждением целей обработки.

4.6. В случае если Учреждение на основании договора поручает обработку персональных данных другому лицу, существенным условием договора должна являться обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

5. Обработка персональных данных

5.1. Обработка персональных данных граждан, обратившихся в Учреждение, может осуществляться исключительно в целях осуществления деятельности, указанной в Уставе Учреждения, и в случаях, установленных законодательством Российской Федерации.

5.2. При определении объема и содержания обрабатываемых персональных данных Учреждение должно руководствоваться Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами Российской Федерации.

5.3. Персональные данные субъектов обрабатываются и хранятся в помещениях Учреждения и на учетных машинных носителях в соответствии с «Инструкцией по учету машинных носителей».

5.4. Персональные данные субъектов могут быть получены, обработаны и переданы на хранение как на бумажных носителях, так и в электронном виде – в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

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

5.5.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы), должны содержать:

5.5.1.1. сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

5.5.1.2. имя (наименование) и адрес Учреждения;

5.5.1.3. фамилию, имя, отчество и адрес субъекта персональных данных;

5.5.1.4. источник получения персональных данных;

5.5.1.5. сроки обработки персональных данных;

5.5.1.6. перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

5.5.1.7. общее описание используемых Учреждением способов обработки персональных данных;

5.5.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, в тех случаях, когда существует необходимость получения письменного согласия на обработку персональных данных;

5.5.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

5.5.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.6. При ведении журналов (реестров, книг) без использования средств автоматизации, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Учреждение, или в иных аналогичных целях, должны соблюдаться следующие условия:

5.6.1. необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Учреждения, содержащим:

5.6.1.1. сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

5.6.1.2. способы фиксации и состав информации, запрашиваемой у субъектов персональных данных;

5.6.1.3. перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги);

5.6.1.4. сроки обработки персональных данных;

5.6.1.5. сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Учреждение, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

5.6.2. копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

5.6.3. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Учреждение.

5.7. При обработке персональных данных допущенные к ним лица обязаны соблюдать нижеперечисленные требования:

5.7.1. Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда субъектам персональных данных, затруднения реализации прав и свобод граждан Российской Федерации.

5.7.2. Работники должны быть ознакомлены под расписку с нормативными документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

5.7.3. Субъекты персональных данных, не являющиеся работниками Учреждения, имеют право ознакомиться с нормативными документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

5.7.4. В случае выявления недостоверных персональных данных субъекта или неправомерных действий с ними работников Учреждения при обращении или по запросу гражданина, являющегося субъектом персональных данных, или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, необходимо осуществить блокирование персональных данных, относящихся к соответствующему гражданину, с момента такого обращения или получения такого запроса на период проверки.

5.7.5. В случае подтверждения факта недостоверности персональных данных на основании документов, представленных субъектом персональных данных, или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов необходимо уточнить персональные данные и снять их блокирование.

5.7.6. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, необходимо устранить допущенные нарушения. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, – также указанный орган.

5.8. Получение персональных данных

5.8.1. Учреждение не имеет права получать и обрабатывать персональные данные работников Учреждения и других субъектов персональных данных об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, кроме случаев, когда субъект персональных данных дал согласие в письменной форме с указанием данных категорий персональных данных.

5.8.2. Персональные данные следует получать лично у субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку Учреждением в случаях предусмотренных законодательством Российской Федерации. Форма заявления субъекта на обработку персональных данных представлена в Приложении 1 к настоящему Положению.

5.8.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Форма отзыва согласия на обработку персональных данных представлена в Приложении 2 к настоящему Положению.

5.8.4. В случае возникновения необходимости получения персональных данных у третьей стороны следует известить об этом субъекта заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных. Форма заявления субъекта на получение его персональных данных от третьей стороны представлена в Приложении 3 к настоящему Положению.

5.8.5. Работник Учреждения должен сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

5.8.6. Работник Учреждения должен проверять достоверность персональных данных, сверяя данные, предоставленные субъектом или его законным представителем, с имеющимися у субъекта или его законного представителя документами.

5.8.7. При принятии решений, затрагивающих интересы субъекта персональных данных, не допускается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.9. Хранение персональных данных

5.9.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.9.2. Хранение персональных данных субъектов осуществляется на бумажных и электронных носителях, доступ к которым ограничен.

5.9.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях без использования средств автоматизации.

5.9.4. Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа или металлического шкафа, обеспечивающего защиту от несанкционированного доступа.

5.9.5. Работники, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно "Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденному постановлением Правительства Российской Федерации 15 сентября 2008 г. № 687.

5.9.6. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

5.10. При передаче персональных данных субъекта Учреждение обязано соблюдать нижеперечисленные требования:

5.10.1. Передавать персональные данные субъектов допускается только тем работникам, которые имеют допуск к обработке персональных данных.

5.10.2. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами. Форма заявления субъекта на передачу его персональных данных третьей стороне представлена в Приложении 4 настоящего Положения.

5.10.3. Предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности.

5.10.4. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

5.10.5. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции. Информация запрашивается с письменного согласия субъекта персональных данных.

5.10.6. Передавать персональные данные субъекта представителям субъектов в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

5.10.7. Все сведения о передаче персональных данных субъекта регистрируются в Журнале учета запросов от сторонних лиц в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также перечень переданной информации. Форма журнала представлена в Приложении 5 к настоящему Положению.

5.10.8. Сведения о выдаче ответов на обращения граждан регистрируются в Журнале учета обращений граждан. Форма журнала представлена в Приложении 6 к настоящему Положению.

5.11. Конфиденциальность персональных данных

5.11.1. Учреждение обеспечивает конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных.

5.11.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (машинные) носители информации.

5.11.3. Все работники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных представлена в Приложении 7 настоящего Положения.

5.12. Уничтожение персональных данных

5.12.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.12.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством Российской Федерации, а также нормативными документами Учреждения.

5.12.3. Уничтожение носителей информации (как бумажных, так и машинных) производится по решению Главного врача Учреждения.

5.12.4. Вывод из эксплуатации машинного носителя производится путем его форматирования, либо путем его механического повреждения в присутствии ответственного за обеспечение безопасности персональных данных.

5.12.5. Бумажные носители персональных данных уничтожаются в бумагорезательной машине, а также путем сжигания.

5.12.6. По факту уничтожения персональных данных составляется акт, утверждаемый Главным врачом Учреждения, и делается отметка в соответствующем журнале. Форма акта представлена в Приложении 8 настоящего Положения.

6. Права и обязанности субъектов персональных данных и учреждения

6.1. В целях обеспечения защиты персональных данных субъекты имеют право:

6.1.1. получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

6.1.2. осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

6.1.3. требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации;

6.1.4. при отказе Учреждения или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

6.1.5. дополнить персональные данные оценочного характера заявлением, выражающим собственную точку зрения;

6.1.6. требовать от Учреждения или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

6.1.7. обжаловать в судебном порядке любые неправомерные действия или бездействие Учреждения или уполномоченного им лица при обработке и защите персональных данных субъекта.

6.2. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

6.3. Для защиты персональных данных субъектов Учреждение:

6.3.1. обеспечивает защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;

6.3.2. производит ознакомление субъекта или его представителей с настоящим Положением и его правами в области защиты персональных данных под расписку;

6.3.3. по запросу производит ознакомление субъекта персональных данных, не являющегося работником, или в случае недееспособности субъекта, его законных представителей с настоящим Положением и его правами в области защиты персональных данных;

6.3.4. осуществляет передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

6.3.5. предоставляет персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим положением и законодательством Российской Федерации;

6.3.6. обеспечивает субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

6.3.7. по требованию субъекта или его законного представителя предоставляет ему информацию о его персональных данных и обработке этих данных.

7. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением за счет своих средств, если иное не предусмотрено законодательством РФ.

7.2. В Учреждении защите подлежат все сведения, содержащие персональные данные субъектов, в том числе:

7.2.1. зафиксированные в бумажных документах;

7.2.2. зафиксированные в электронных документах на технических средствах, включая внешние носители;

7.2.3. речевая (акустическая) информация, содержащая персональные данные;

7.2.4. текстовая и графическая видовая информация, содержащая персональные данные;

7.2.5. информация, представленная в виде информативных электрических сигналов, физических полей, содержащая персональные данные.

7.3. Защита персональных данных должна вестись по трем взаимодополняющим направлениям:

7.3.1. Проведение организационных мероприятий:

7.3.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

7.3.1.2. ознакомление работников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

7.3.1.3. проведение обучения работников вопросам защиты персональных данных.

7.3.2. Программно-аппаратная защита:

7.3.2.1. разработка модели угроз безопасности персональных данных;

7.3.2.2. внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия;

7.3.2.3. организация учета носителей персональных данных.

7.3.3. Инженерно-техническая защита:

7.3.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

7.3.3.2. установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

7.4. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за обеспечение безопасности персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Учреждения.

7.5. Организацию и контроль защиты персональных данных в Учреждении осуществляет ответственный за организацию обработки персональных данных Учреждения.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

8.1. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

8.2. Главный врач Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

8.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) Учреждения,

влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

8.4. Работник Учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

8.5. Кодексом Российской Федерации об административных правонарушениях предусмотрены следующие составы административных правонарушений:

8.5.1. статья 5.27. Нарушение законодательства о труде и об охране труда;

8.5.2. статья 5.39. Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации;

8.5.3. статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

8.5.4. часть 2 статья 13.12. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну);

8.5.5. статья 13.14. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 Кодекса;

8.5.6. часть 1 статья 19.5. Невыполнение в установленный срок законного предписания законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства (Роскомнадзор);

8.5.7. статья 19.7. Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде (уведомление Роскомнадзора).

8.6. Уголовным кодексом Российской Федерации предусмотрены следующие преступления в области персональных данных:

8.6.1. часть 1 статьи 137. Незаконное собирание или распространение персональных данных либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации;

8.6.2. часть 2 статьи 137. Те же деяния, совершенные лицом с использованием своего служебного положения;

8.6.3. статья 140. Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан;

8.6.4. статья 272. Неправомерный доступ к охраняемой законом компьютерной информации (в т.ч. к персональным данным).

8.7. В соответствии с Трудовым кодексом Российской Федерации:

8.7.1. статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника;

8.7.2. статья 192. За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить ... дисциплинарные взыскания;

8.7.3. по инициативе работодателя может быть расторгнут трудовой договор в случае разглашения персональных данных другого работника (пп в п. 6 ст. 81 ТК РФ).