

## ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

**1.1** Настоящее положение разработано в целях обеспечения реализации требований законодательства Российской Федерации в области обработки и защиты персональных данных;

**1.2** Настоящее положение регулирует отношения, связанные с обработкой персональных данных, включающие в себя производимые ООО «Новодента+» действия с использованием средств автоматизации или без использования таких средств по сбору, записи, систематизации, накоплению, уточнению (обновлению, изменению), извлечению, получению, хранению, комбинированию, использованию, передаче сведений, отнесенных законодательством Российской Федерации к персональным данным, с целью защиты прав и свобод человека и гражданина (субъекта персональных данных) при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную, семейную и врачебную тайну;

**1.3** Настоящее положение - общедоступный документ, декларирующий концептуальные основы деятельности ООО «Новодента+» при обработке персональных данных, раскрывающий:

- категории персональных данных, обрабатываемых в ООО «Новодента+»;
- цели, способы и принципы обработки персональных данных;
- права и обязанности работников ООО «Новодента+» и субъектов персональных данных при обработке персональных данных;
- перечень мер, обеспечивающих безопасность персональных данных;

**1.4** Настоящее положение вступает в силу с момента его утверждения приказом генерального директора, и является обязательным для исполнения всеми работниками ООО «Новодента+».

### 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**2.1** В настоящем положении использованы следующие термины и определения:

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

**Биометрические персональные данные** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных,

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

**Врачебная тайна** - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, а также иные данные, полученные при его медицинском обследовании и лечении;

**Генеральный директор** – генеральный директор ООО «Новодента+»;

**Документ (документированная информация)** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

**Документ, содержащий персональные данные пациента** – документ, необходимый для осуществления действий в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, а также для оформления договорных отношений;

**Документ, содержащий персональные данные работника** – документ, предоставляемый работником работодателю (оператору) в связи с трудовыми отношениями и касающийся конкретного субъекта персональных данных, а также иной документ, содержащий сведения, предназначенные для использования в служебных целях;

**Должностное лицо** - лицо, наделенное определенными обязанностями и полномочиями в соответствии с учредительными документами и внутренними правилами Общества;

**Доступ к информации** - возможность получения информации и (или) ее использования;

**Здоровье** - состояние физического, психического и социального благополучия человека, при котором отсутствуют заболевания, а также расстройства функций органов и систем организма;

**Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации или без использования таких средств;

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

**Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом условие не раскрывать и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законом;

**Медицинская помощь** - комплекс мероприятий, направленных на поддержание и (или) восстановление здоровья и включающих в себя предоставление медицинских услуг;

**Медицинская организация** - юридическое лицо независимо от организационно-правовой формы, осуществляющее в качестве основного (уставного) вида деятельности медицинскую деятельность на основании лицензии, выданной в порядке, установленном законодательством Российской Федерации. Также к медицинским организациям приравниваются индивидуальные предприниматели, осуществляющие медицинскую деятельность наряду с основной (уставной) деятельностью;

**Медицинская услуга** - медицинское вмешательство или комплекс медицинских вмешательств, направленных на профилактику, диагностику и лечение заболеваний, медицинскую реабилитацию и имеющих самостоятельное законченное значение;

**Медицинский работник** - физическое лицо, которое имеет медицинское или иное образование, работает в медицинской организации и в трудовые (должностные) обязанности которого входит осуществление медицинской деятельности, либо физическое лицо, которое является индивидуальным предпринимателем, непосредственно осуществляющим медицинскую деятельность;

**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;

**Общедоступные персональные данные** - персональные данные, к которым доступ неограниченного круга лиц предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

**Общество (работодатель, оператор)** – ООО «Новодента»;

**Оператор** - 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;

**Ответственность** - ответственность, установленная в соответствии с требованиями действующих локальных нормативных актов Общества и Законодательством РФ;

**Пациент** - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

**Персональные данные** - любая информация, относящаяся прямо или косвенно к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество; год, месяц, дата и место рождения; адрес; семейное, социальное, имущественное положение; образование; профессия; доходы; другая информация;

**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

**Работник** – физическое лицо, состоящее в трудовых и иных гражданско-правовых отношениях с ООО «Новодента»;

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**Субъект** - субъект персональных данных (работник, пациент);

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

### 3. НОРМАТИВНЫЕ ССЫЛКИ

- Конституция Российской Федерации, принята всенародным голосованием 12.12.1993 г.;
- Федеральный закон РФ от 30.11.1994 г. № 51-ФЗ «Гражданский кодекс Российской Федерации»;
- Федеральный закон РФ от 30.03.1999 г. № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»;
- Федеральный закон РФ от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации»;

- Федеральный закон РФ от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон РФ от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон РФ от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральный закон РФ от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства РФ от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена Заместителем директора ФСТЭК 15.02.2008 г.;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена Заместителем директора ФСТЭК от 14.02.2008 г.;
- Приказ ФСТЭК РФ от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Госстандарта России от 27.02.1998 г. № 28 «ГОСТ Р 51141-98 Государственный стандарт Российской Федерации. Делопроизводство и архивное дело. Термины и определения»;
- Лицензия Департамента здравоохранения г. Москвы № ЛО-77-01-001619 от 28.07.2009 г. на осуществление медицинской деятельности;
- Устав Общества;
- Правила внутреннего трудового распорядка, утвержденные генеральным директором Общества 01.10.2007 г.

## 4. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

**4.1** Оператором, организующим и осуществляющим обработку персональных данных, является ООО «Новодента+».

**4.2** К персональным данным относится информация, относящаяся прямо или косвенно к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

- сведения, сообщенные работником работодателю при приеме на работу, а также полученные и образованные в процессе трудовой деятельности субъекта;
- информация, касающаяся состояния здоровья пациента;
- биометрические сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных.

### **4.3 Состав персональных данных**

Перечень документов и материалов, составляющих персональные данные, обрабатываемых в Обществе:

#### **4.3.1** Документы и их копии:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка (за исключением случаев совместительства или приема на работу впервые);
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика (по желанию работника);
- воинского учета (для военнообязанных лиц и лиц, подлежащих призыву на военную службу);
- об образовании, профессии, квалификации или наличии специальных знаний или специальной подготовки;
- о составе семьи работника;
- о состоянии здоровья работника (если в соответствии с законодательством он должен пройти периодический и предварительный медицинский осмотры, а также в случае временной нетрудоспособности);
- подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;
- о беременности работницы и возрасте детей для предоставления матери установленных законом условий труда, гарантий и компенсаций;

#### **4.3.2** Материалы кадрового делопроизводства (сведения, внесенные в учетные формы на бумажных и электронных носителях):

- трудовой договор;
- «Личная карточка работника», в которой отражаются анкетные и биографические данные, а также сведения о переводах на другую работу; об аттестации; о допуске к государственной тайне, работе с конфиденциальной информацией и персональными данными; о повышении квалификации; о профессиональной переподготовке; о наградах (поощрениях), почетных званиях; об отпусках; о социальных гарантиях; о месте жительства и контактных телефонах;
- приказы по личному составу - прием на работу, изменение условий трудового договора, его прекращение, а также приказы (распоряжения о поощрениях и дисциплинарных взысканиях, примененных к работнику);
- основания к приказам по личному составу;
- личные дела;
- сведения об имуществе;

- документы, содержащие сведения о заработной плате, за исключением сведений о системе оплаты труда;
- документы, содержащие сведения по страхованию работников Общества, в том числе суммы страхования и размер страховых премий, перечисленных Обществом в страховую компанию (при наличии);
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, муниципальные и другие учреждения;
- справочно-информационный банк данных (учетный аппарат) по персоналу - картотеки, журналы, базы данных и др.;
- телефонный справочник, в том числе списки электронных адресов работников.

**4.3.3** Документы и материалы, связанные с взаимоотношениями Общества и пациента (на бумажных и электронных носителях):

- фамилия, имя, отчество;
- день, месяц, год рождения;
- данные о гражданстве;
- данные об образовании (при необходимости);
- сведения о периодах и видах трудовой деятельности (при необходимости);
- адрес постоянной регистрации и фактического проживания, номер домашнего телефона (телефона сотовой связи);
- данные паспорта или иного документа, удостоверяющего личность;
- данные страхового полиса;
- данные о состоянии здоровья пациента, полученные надлежащим образом и(или) предоставленные им;
- биометрические данные пациента;
- данные о проведенных медицинских исследованиях (оказанной медицинской помощи);
- данные об оказанных медицинских услугах и их результат.

## **5. ИСТОЧНИКИ И СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**5.1** Получение персональных данных преимущественно осуществляется путем представления их самим пациентом (законным представителем) или работником за исключением случаев прямо предусмотренных законодательством РФ.

**5.2** В целях информационного обеспечения в Обществе могут создаваться общедоступные источники персональных данных субъектов персональных данных, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты и иные персональные данные, сообщаемые субъектом персональных данных.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных, уполномоченного органа по защите прав субъектов персональных данных либо по решению суда.

**5.3** В случае необходимости проверки или получения дополнительных персональных данных пациента или работника Общество заблаговременно сообщает субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа пациента или работника дать письменное согласие на их получение.

**5.4** К субъектам персональных данных относятся:

- работники Общества;

- кандидаты для приема на работу;
- уволенные работники;
- контрагенты (индивидуальные предприниматели, физические лица, исполнительные органы юридических лиц);
- учредители;
- пациенты.

## 6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных осуществляется во исполнение соблюдения требований законов и иных нормативных правовых актов, с целью содействия субъектам персональных данных в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, контроля за состоянием здоровья пациентов, рассмотрению вопросов и принятию соответствующих решений об оказании медицинской помощи и медицинских услуг.

### 6.1 Обработка персональных данных осуществляется:

- без использования средств автоматизации (в части использования и хранения отдельных документов, а также иной информации, составляющей персональные данные субъекта);
- с использованием автоматизированной информационной системы (в части формирования информационных ресурсов на основе получения, хранения, уточнения (обновления, изменения), комбинирования, документирования информации о конкретном субъекте).

### 6.2 Принципы обработки персональных данных:

Обработка персональных данных осуществляется на основе следующих принципов:

- законности и справедливой основы;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки персональных данных, избыточных по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;
- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Оператором допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

### 6.3 Условия обработки персональных данных:

Оператор производит обработку персональных данных при наличии хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

#### **6.4 Требования, предъявляемые к обработке персональных данных пациента и работника**

**6.4.1** Обработка персональных данных пациента осуществляется исключительно в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, оформления договорных отношений с пациентом при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну в соответствии с законодательством Российской Федерации, или иным уполномоченным на то работником;

**6.4.2** Обработка персональных данных работников осуществляется с целью, оформления трудовых отношений, расчета и выдачи заработной платы и иных выплат, налоговых и пенсионных отчислений, содействия в трудоустройстве, обучении, повышении квалификации и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества работодателя;

**6.4.3** Персональные данные пациента получают у него самого или у его полномочного представителя. Персональные данные работника работодатель получает у него самого. Если персональные данные пациента или работника возможно, получить только у третьей стороны, то пациент или работник уведомляются об этом заранее и от него должно быть получено письменное согласие;

**6.4.4** Запрещена обработка персональных данных пациента и работника, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев предусмотренных законодательством РФ. В случаях, непосредственно связанных с вопросами трудовых отношений, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

**6.4.5** Запрещается принятие решений, основанных исключительно на автоматизированной обработке персональных данных, порождающих юридические

последствия в отношении пациента и работника или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством РФ.

## **6.5 Особенности обработки персональных данных, осуществляемой без использования средств автоматизации**

**6.5.1** Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

**6.5.2** Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее;

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

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель;

**6.5.4** При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (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;

б) 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, - при необходимости получения письменного согласия на обработку персональных данных;

в) 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;

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

**6.5.5** 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 отдельной обработки персональных данных, в частности:

а) 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;

б) 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.

**6.5.6** Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

**6.5.7** Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

## **6.6 Обработка биометрических персональных данных**

Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

## **6.7 Обработка персональных данных третьими лицами**

Общество вправе поручить обработку персональных данных другому лицу с согласия пациента, если иное не предусмотрено законодательством РФ, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».

**6.7.1** В поручении оператора должны быть определены:

- перечень действий (операций) с персональными данными, которые должны быть совершены лицом, осуществляющим обработку персональных данных;
- цели обработки;
- обязанность лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке;
- требования к защите обрабатываемых персональных данных в соответствии с законодательством РФ.

**6.7.2** Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие пациента (работника) на обработку его персональных данных.

В случае если оператор поручает обработку персональных данных другому лицу, ответственность перед пациентом (работником) за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

## **7. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**7.1** Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации. От работников, ответственных за хранение персональных данных, а также работников, владеющих персональными данными в силу своих должностных обязанностей, берутся обязательства о неразглашении персональных данных.

**7.2** Обеспечения конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

## **8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ**

**8.1 Внутренний доступ:** Право доступа к персональным данным субъекта (с его письменного согласия) внутри Общества, кроме случаев, когда такое согласие не требуется по законодательству РФ, имеют:

- должностные лица Общества при выполнении ими своих служебных обязанностей. Данным категориям работников в их должностные обязанности включается пункт об обязанности соблюдения требований по защите персональных данных.

- сам субъект персональных данных, носитель данных;

Документы, содержащие персональные данные, за пределы помещения их хранения не выносятся, за исключением случаев выдачи их генеральному директору или иному руководителю Общества с согласия генерального директора. Копирование документов осуществляется уполномоченным на то работником.

**8.2 Внешний доступ:** К числу массовых потребителей персональных данных вне Общества относятся:

- государственные и негосударственные функциональные структуры (налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; муниципальные органы управления);

- надзорно-контрольные органы (имеют доступ к информации только в сфере своей компетенции);

- родственники и члены семей.

Сведения о работающем или уже уволенном работнике могут быть предоставлены внешней организации только с письменного запроса (на бланке организации), с приложением копии нотариально заверенного заявления работника о согласии предоставления персональных данных;

Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника;

В случае развода бывшая супруга (супруг) имеют право обратиться в Общество с письменным запросом о размере заработной платы работника без его согласия в соответствии с законодательством РФ.

## 9. ПОРЯДОК ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Использование персональных данных возможно только в соответствии с целями, определившими их получение.

**9.1** Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение на бумажных носителях, в электронном виде, с помощью локальной компьютерной сети и соответствующей компьютерной программы, используемой в Обществе.

**9.2** Персональные данные пациентов хранятся в бумажном (договор, согласие на обработку персональных данных, амбулаторная карта, бланки направлений, результаты обследований, перечень оказанных медицинских услуг, и т.д.) и электронном виде. В электронном виде персональные данные пациентов хранятся в информационной системе персональных данных Общества, а также в их архивных копиях.

**9.3** Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

**9.4** Все документы, носители информации на магнитной или оптической основе и дела со сведениями конфиденциального характера, хранятся в надежно запираемых шкафах в служебных помещениях, доступ посторонних лиц в которые исключен;

**9.5** Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено.

### **9.6 Уточнение, блокирование и уничтожение персональных данных**

**9.6.1** Целью уточнения персональных данных, в том числе обновления и изменения, является обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемых Обществом. Уточнение персональных данных осуществляется оператором по собственной инициативе, по требованию субъекта персональных данных или его представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случаях, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными.

**9.6.2** Целью блокирования персональных данных является временное прекращение обработки персональных данных до момента устранения обстоятельств, послуживших основанием для блокирования персональных данных.

Блокирование персональных данных осуществляется Обществом по требованию субъекта персональных данных или его представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними.

**9.6.3** Уничтожение персональных данных производится:

- по достижении цели обработки персональных данных;
- в случае утраты необходимости в достижении целей обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения департаментом неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

**9.7** При уничтожении материальных носителей персональных данных составляется Акт об уничтожении носителей, содержащих персональные данные.

## **10. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ**

**10.1** Передача персональных данных возможна только с письменного согласия субъекта персональных данных или без такового в случаях, прямо предусмотренных законодательством РФ;

**10.2** Предоставление персональных данных пациентов третьим лицам без письменного согласия пациента, возможно если:

- передача необходима для защиты жизни и здоровья пациента, либо других лиц, и получение его согласия невозможно;
- в целях обследования и лечения пациента, не способного из-за своего состояния выразить свою волю;
- в случае оказания помощи несовершеннолетнему в возрасте до 15 лет, для информирования его родителей или законных представителей;
- при наличии оснований, позволяющих полагать, что права и интересы пациента могут быть нарушены противоправными действиями других лиц;
- по мотивированному запросу судебных органов в связи с осуществлением правосудия, правоохранительных и иных государственных организаций в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

**10.3** Не допускается сообщать персональные данные в коммерческих целях без письменного согласия субъекта персональных данных. Обработка персональных данных субъекта персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

**10.4** Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону, факсу, электронной почте.

**10.5** Запрещается запрашивать и передавать информацию о состоянии здоровья субъекта персональных данных, за исключением сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

**10.6** При передаче персональных данных третьим лицам, в том числе представителям работников, в порядке, установленном Трудовым кодексом РФ и настоящим Положением, работодатель имеет право передавать и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения третьими лицами их функций.

Факт передачи персональных данных пациентов и работников Общества третьим лицам фиксируется в Журнале учета выданных персональных данных, в котором регистрируются поступившие запросы, сведения о лице, направившем запрос, дата передачи персональных данных, а также указывается вид выданной информации;

В случае если лицо, обратившееся с запросом, не уполномочено в соответствии с федеральным законодательством на получение персональных данных пациента или работника, либо отсутствует письменное согласие пациента или работника на передачу его персональных данных, оператор обязан отказать в предоставлении персональных данных с выдачей мотивированного отказа в предоставлении персональных данных в письменной форме, копия которого с отметкой о его получении (отправке) хранится в Обществе.

**10.7** Не допускается разглашение и(или) передача сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных и иных обязанностей;

## **11. ЗАЩИТА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**11.1** Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

**11.2** Защита персональных данных представляет собой строго регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Общества.

Защита персональных данных от неправомерного их использования или утраты обеспечивается за счет его средств Общества, в порядке, установленном федеральными законами.

**11.3 Обеспечение безопасности персональных данных достигается:**

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

**11.4 Обеспечение безопасности персональных данных при их обработке в информационных системах**

Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора.

**11.4.1** В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

**11.5** При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

**11.6** Для обеспечения внешней защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для постороннего лица, пытающегося совершить несанкционированный доступ и овладение информацией.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Общества. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих персональные данные.

**11.7** Для обеспечения внешней защиты персональных данных работники Общества обязаны строго и неукоснительно соблюдать:

- порядок приема, учета и контроля деятельности посетителей (пациентов);
- пропускной режим;
- порядок использования технические средства охраны и сигнализации;
- требования к защите информации при интервьюировании и беседах.

## **12. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

Закрепление прав работника и пациента, регламентирующих защиту их персональных данных, обеспечивает сохранность полной и точной информации о них.

**12.1** Ознакомление с документами Общества, устанавливающими порядок обработки персональных данных, а также о правах и обязанностях субъектов

персональных данных является обязанностью работников Общества, но правом пациентов.

**12.2** В целях защиты персональных данных, хранящихся в Обществе, субъекты имеют право:

- на полную информацию об их персональных данных и обработке этих данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной, семейной тайны, врачебной и иной тайны;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неверными, неполными, устаревшими, недостоверными, незаконно полученными или не являющимися необходимыми для заявленной цели обработки;
- требовать извещения работодателем (медицинской организацией) всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке любые неправомерные действия (бездействия) работодателя (медицинской организации) при обработке и защите его персональных данных.

**12.3** Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

**12.4** Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

**12.5** Субъект персональных данных имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

**12.6 Работник обязан:**

- передавать работодателю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать работодателю об изменении своих персональных данных (об образовании, профессии, специальности, присвоении нового разряда и пр.), и представлять подтверждающие документы, для внесения изменений в трудовую книжку и другую кадровую документацию.

**12.7** С целью своевременной и полной реализации своих прав при обращении в Общество за медицинской помощью (услугой) **пациент обязан:**

- сообщить работникам о наличии заболеваний, представляющих опасность для здоровья населения, вируса иммунодефицита человека;
- информировать работников о ранее выявленных медицинских противопоказаниях к применению лекарственных средств, наследственных и перенесенных заболеваниях, об обращениях за медицинской помощью, а также об изменениях в состоянии здоровья.

**12.8 Права субъекта персональных данных и обязанности оператора персональных данных**

В случае если сведения, а также обрабатываемые персональные данные, были предоставлены для ознакомления пациенту по его запросу, пациент вправе обратиться повторно в Общество или направить повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

В случае выявления неправомерной обработки персональных данных при обращении пациента или его представителя либо по запросу пациента или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении пациента или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы пациента или третьих лиц.

В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных пациентом или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой оператором (или лицом, действующим по поручению оператора), оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, оператор 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 оператор обязан уведомить пациента или его представителя, а в случае, если обращение пациента или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является пациент, иным соглашением между оператором и пациентом, либо если оператор не вправе осуществлять обработку персональных данных без согласия пациента на основаниях, предусмотренных законодательством РФ.

В случае отзыва пациентом согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и пациентом, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством РФ. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законодательством.

### **13. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОРЯДКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**13.1** Контроль исполнения требований настоящего Положения и ответственность за его поддержание в актуальном состоянии возлагается на генерального директора.

**13.2** Лицо, ответственное за организацию обработки персональных данных, обязано:

- осуществлять внутренний контроль за соблюдением в Обществе законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Общества положения законодательства Российской Федерации о персональных данных, локальных нормативных актов по вопросам обработки и защиты персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и(или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

**13.3** Работники, допустившие нарушения требований настоящего Положения, в зависимости степени нарушения и характера причиненного вреда, несут ответственность предусмотренную уголовным, трудовым, гражданско-правовым и иным законодательством Российской Федерации.