

**ПОЛОЖЕНИЕ**  
**О ПОРЯДКЕ ОРГАНИЗАЦИИ ОБРАБОТКИ И**  
**ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ**  
**СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО**  
**УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ «ЛУНИНСКАЯ РАЙОННАЯ БОЛЬНИЦА»**

**НАЗНАЧЕНИЕ**

**1.1. Положение о порядке организации обработки и обеспечении безопасности персональных данных в информационных системах персональных данных Государственного бюджетного учреждения здравоохранения «Лунинская районная больница» (далее Документ) — документ, определяющий политику Государственного бюджетного учреждения здравоохранения «Лунинская районная больница» (далее ГБУЗ «Лунинская РБ») в отношении обработки персональных данных (далее — ПДн), содержащий сведения о реализуемых требованиях к защите персональных данных.**

1.2. Настоящий документ разработан на основании: статей Конституции Российской Федерации, Федерального закона от 30.11.1994 №51-ФЗ «Гражданский кодекс Российской Федерации», Федерального закона от 30.12.2001 №197-ФЗ «Трудовой кодекс Российской Федерации», Федерального закона от 31.07.1998 № 146-ФЗ «Налоговый кодекс Российской Федерации»; Федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федерального закона от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федерального закона от 01.04.1996 №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119, Постановления Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ РФ от 10.07.2014 №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.3. Настоящий Документ разработан на основании: приказа от 10.01.2017г. № 2 «Об утверждении Положения о защите персональных данных в ГБУЗ «Лунинская районная больница»

1.4. Целью настоящего Документа является исполнение законодательства Российской Федерации в области обработки персональных данных субъектов персональных данных.

**1.5.** Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением.

## **2. ОБЩИЕ ПОЛОЖЕНИЯ**

**2.1.** Настоящий Документ является общедоступным документом, декларирующим основы деятельности ГБУЗ «Лунинская РБ» при обработке персональных данных.

**2.2.** Настоящим Документом определяется порядок обращения с персональными данными пациентов ГБУЗ «Лунинская РБ» и персональными данными работников (субъектов персональных данных) ГБУЗ «Лунинская РБ».

**2.3.** Защита персональных данных, используемых при обработке персональных данных, осуществляемой в ГБУЗ «Лунинская РБ» от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них, обеспечивается ГБУЗ «Лунинская РБ» за счет средств ГБУЗ «Лунинская РБ» в порядке, установленном Федеральным Законом и другими нормативными документами Российской Федерации.

**2.4.** В случаях, не указанных в настоящем Документе, следует руководствоваться действующими федеральными законами и нормативными правовыми актами Российской Федерации, регулирующими порядок обработки персональных данных.

## **3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**3.1.** Учреждение обрабатывает персональные данные пациента исключительно в следующих целях:

**3.1.1.** Исполнения положений нормативных актов, указанных в п.1.2. настоящего Документа.

**3.1.2.** Предоставления субъектам персональных данных квалифицированной медицинской помощи, учета результатов договорных обязательств, а также наиболее полного исполнения учреждением обязательств и компетенций в соответствии с Федеральным законом «Об обязательном медицинском страховании граждан в Российской Федерации» от 29 ноября 2010 года № 326-ФЗ и Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ.

**3.2.** Обработка персональных данных пациентов ГБУЗ «Лунинская РБ» осуществляется для решения следующих задач:

- Осуществление расчетов с ФОМС и страховыми организациями за оказание медицинских услуг застрахованным лицам;
- Формирования отчетов о результатах деятельности;
- Назначение и начисление счетов на оказание услуг и иных выплат;
- Обработка медицинских карт (в т.ч. в электронной форме);
- Поддержание контактов с законными представителями субъекта персональных данных;
- Проведение лечебно-профилактических мероприятий;
- Иные задачи, необходимые для повышения качества и эффективности деятельности ГБУЗ «Лунинская РБ».

**3.3.** Учреждение обрабатывает персональные данные работника исключительно в следующих целях:

- 3.3.1.** Исполнения положений нормативных актов, указанных в п.1.2. настоящего Документа.
- 3.3.2.** Принятие решения о трудоустройстве соискателя.
- 3.3.3.** Заключение и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера, содействие в обучении и продвижении по службе, контроля количества и качества выполняемой работы.
- 3.4.** Обработка персональных данных сотрудников ГБУЗ «Лунинская РБ» осуществляется для решения следующих задач:
- 3.4.1.** Оформление трудоустройства соискателя.
- 3.4.2.** Начисление заработной платы и иных, предусмотренных законодательством РФ выплат.
- 3.4.3.** Ведение кадрового учета, а именно учета:
- повышения квалификаций;
  - полученного образования;
  - прохождения аттестаций;
  - отпусков;
  - больничных листов;
  - регистраций особых условий труда;
  - получение научных степеней и званий;
  - получение наград и поощрений;
  - получение социальных льгот;
  - регистраций места жительства;
  - иных событий кадрового учета, предусмотренных законодательством РФ.
- 3.4.4.** Военный учет.
- 3.4.5.** Контроль количества и качества выполняемой работы.

#### **4. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**4.1.** Обработка и хранение персональных данных должны осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

#### **5. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Информация о персональных данных собирается исключительно с письменного согласия на обработку персональных данных субъекта персональных данных или его законного представителя, за исключением случаев прямо предусмотренных действующим законодательством РФ. При отказе субъекта персональных данных дать письменное согласие ему объясняются последствия такого отказа.

Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях.

##### **5.1. Персональные данные пациента**

**5.1.1.** В состав персональных данных пациентов Учреждения входит следующая информация: фамилия, имя, отчество, год, месяц, дата и место рождения, серия и номер

паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное положение, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса и его действительность, номер амбулаторной карты, номер истории болезни, сведения о состоянии здоровья, в том числе группа здоровья, группа инвалидности и степень ограничения к трудовой деятельности, состояние диспансерного учета, зарегистрированные диагнозы по результатам обращения пациентов к врачу, в том числе при прохождении диспансеризации и медицинских осмотров, информация об оказанных медицинских услугах, в том числе о проведенных лабораторных анализах и исследованиях и их результатах, выполненных оперативных вмешательствах, случаях стационарного лечения и их результатах, о выданных листах временной нетрудоспособности с указанием номера листа нетрудоспособности и периода нетрудоспособности, регистрация прикрепления на территории обслуживания пациента – дата и признак прикрепления, информация о выписанных и отпущенных лекарственных средствах и изделиях медицинского назначения, информация о наличии льгот (по категориям), о документах, подтверждающих право на льготу и право на льготное лекарственное обеспечение, дата и причина смерти гражданина в случае его смерти.

**5.1.2.** Пациент, как субъект персональных данных, в том числе специальной категории персональных данных, имеет право на получение сведений:

- об Операторе, о месте нахождения Оператора;
- о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных;
- на подтверждение факта обработки персональных данных Оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые Оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

**5.1.3.** Пациент также имеет право:

- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- доступа к своим персональным данным при личном обращении к представителю Оператора при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

## **5.2 Персональные данные работника**

**5.2.1.** К персональным данным работника Учреждения относится следующая информация: информация, содержащаяся в трудовой книжке, информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования, информация об образовании, квалификации или о наличии специальных знаний и подготовки, информация, содержащаяся в документах воинского учета, информация медицинского характера, информация, содержащаяся в приказах по личному составу, информация, содержащаяся в иных документах, представляемых работником, содержащих информацию, необходимую работодателю в связи с трудовыми отношениями.

**5.2.2.** 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:

- паспорт или иной документ, удостоверяющий личность;
- 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;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника).

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

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных льготах;
- сведения о месте жительства и контактных телефонах.

**5.2.4.** В кадровом органе создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде: 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 исследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

**5.2.5.** Работник, как субъект персональных данных, имеет право на получение сведений:

- об Операторе, о месте нахождения Оператора,
- о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных,
- на подтверждение факта обработки персональных данных Оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые Оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь а собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

**5.2.6.** Работник имеет право:

- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- доступа к своим персональным данным при личном обращении к представителю Оператора при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

**5.2.7.** Запрещается требовать от лица, поступающего на работу (или прием), документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

**5.3.** Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, дату и место рождения адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Учреждения, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись.

**5.4.** Персональные данные субъектов хранятся в электронных базах данных и на бумажных носителях в помещении отдела кадров Учреждения (регистратуре, архиве, медицинском отделении). Для этого используются специально оборудованные шкафы и сейфы. Личные дела уволенных (прошедших обследование, лечение) субъектов хранятся в архиве Учреждения.

## **6. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧРЕЖДЕНИЯ**

Обработка персональных данных ГБУЗ «Лунинская РБ» осуществляется на основе следующих принципов:

- 6.1.** Учреждение в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона 152-ФЗ «О персональных данных».
- 6.2.** Обработке подлежат только персональные данные, которые отвечают целям их обработки;
- 6.3.** Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

## **7. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ**

**7.1.** Учреждение при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них, а именно:

**7.1.1.** Назначение приказом руководителя Учреждения «О возложении обязанностей по защите информации» ответственных лиц за организацию обработки персональных данных, руководство выполнением работ по комплексной защите информации в учреждении, обеспечение эффективного применения имеющихся организационных и инженерно-технических мер по защите информации, обеспечение контроля за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации и координации деятельности подразделений по защите информации в Учреждении.

**7.1.2.** Помещения, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

**7.1.3.** Доступ к информации в электронном виде должен осуществляться с использованием парольной защиты, а в информационных системах персональных данных — с использованием средств автоматизации в соответствии с нормативными документами.

**7.1.4.** Ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.

**7.1.5** Выбор и реализация методов и способов защиты информации в информационных системах осуществляются на основе определяемых Учреждением угроз безопасности персональных данных (частной модели угроз) и, в зависимости от уровня защищенности информационной системы, определенного в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом ФСТЭК России от 1 ноября 2012 г. №1119. Выбранные и реализованные методы и способы защиты информации в информационных системах должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе системы защиты персональных данных.

**7.1.6.** Выявление фактов несанкционированного доступа к персональным данным и принятие соответствующих мер.

**7.1.7.** Контроль доступа и перемещений работников, пациентов и посетителей Учреждения с помощью систем видеонаблюдения.

**7.1.8.** Соблюдать регламентированную процедуру копирования документов, четко определяющую порядок создания копий на бумажных и электронных носителях и их дальнейшее использование.

**7.1.9.** Информацию, содержащую персональные данные, централизованно хранить на серверах, доступ к которым строго ограничить и регламентировать.

**7.1.10.** Контроль за предпринимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

## **8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**8.1.** Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим российским законодательством.

## **9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

**9.1.** Учреждение имеет право вносить изменения в настоящий документ при изменении действующего законодательства РФ и условий своей деятельности.

Положение является обязательным для исполнения всеми работниками ГБУЗ «Лунинская РБ» имеющими доступ к персональным данным.