

**УТВЕРЖДАЮ**

Главный врач ГБУЗ СК  
«Ессентукский межрайонный  
родильный дом».

\_\_\_\_\_ С.М. Чотчаева

«    » \_\_\_\_\_ 2019 г.

**Политика  
обработки персональных данных и информации подлежащей защите в  
ГБУЗ СК «Ессентукский межрайонный родильный дом».**

Согласовано

Нач. отдела ИТ

Глухов С. С.

Согласовано

Ответственный за  
организацию обработки  
и защиты персональных данных

Панарина Е. В

Согласовано

Юрисконсульт

Иванов С.В.

## **1. Общие положения**

1.1. Настоящая Политика об обработке персональных данных, ГБУЗ СК «Ессентукский межрайонный родильный дом». (далее – Политика):

– является основополагающим внутренним документом ГБУЗ СК «Ессентукский межрайонный родильный дом» (далее – Роддом), регулирующий вопросы обработки персональных данных;

– разработана в целях обеспечения соответствия с законодательством Российской Федерации обработки, хранения и защиты ПДн сотрудников и пациентов Роддома;

– раскрывает основные категории персональных данных, обрабатываемых в Роддоме,

– цели, способы и принципы обработки Роддомом, права и обязанности Роддома при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Роддомом в целях обеспечения безопасности персональных данных при их обработке;

– предназначена для сотрудников Роддома, осуществляющих обработку информации подлежащей защите в целях непосредственной реализации ими закрепленных в Политике принципов, а так же является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Роддома при обработке персональных данных.

## **2. Источники нормативного правового регулирования вопросов обработки персональных данных**

2.1. Политика Роддома в области обработки информации подлежащей защите определяется на основании следующих нормативных правовых актов РФ:

– Конституции Российской Федерации;

- Трудового кодекса Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Налогового кодекса Российской Федерации;
- Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Федерального закона Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановления Правительства России от 15 сентября 2008 г № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных»;
- Приказа ФСТЭК России от 5.02.2010 № 58, зарегистрированного в Минюсте России 19.02.2010 № 16456 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

2.2. Во исполнение настоящей Политики в Роддоме приказами утверждаются следующие локальные нормативные правовые акты:

- Инструкция администратора информационной безопасности информационных систем персональных данных;
- Инструкция по действиям пользователей информационных систем персональных данных в нештатных ситуациях;
- Инструкция по организации антивирусной защиты информационных систем персональных данных;
- Инструкция по порядку проведения проверок состояния защиты персональных данных;

- План внутренних проверок состояния защиты персональных данных;
- Инструкция Пользователя информационных систем персональных данных;
- Перечень сведений конфиденциального характера в ГБУЗ СК «Ессентукский межрайонный родильный дом»;
- Перечень подлежащих защите персональных данных и данных, содержащих врачебную тайну, в ГБУЗ СК «Ессентукский межрайонный родильный дом»;
- План мероприятий по защите персональных данных;
- Положение о защите персональных данных сотрудников государственного бюджетного учреждения здравоохранения Ставропольского края «Ессентукский межрайонный родильный дом»;
- Положение о защите персональных данных пациентов государственного бюджетного учреждения здравоохранения Ставропольского края «Ессентукский межрайонный родильный дом»;
- Акт классификации информационных систем персональных данных ГБУЗ СК «Ессентукский межрайонный родильный дом»;
- Аналитическое обоснование необходимости создания системы защиты персональных данных информационных систем персональных данных ГБУЗ СК «Ессентукский межрайонный родильный дом»;
- и иные локальные документы Роддома, принимаемые во исполнение требований действующих нормативных правовых актов РФ в области обработки персональных данных.

### **3. Основные термины и понятия, используемые в локальных документах Роддома, принимаемых по вопросу обработки персональных данных**

- **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и

место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем сведений конфиденциального характера в ГБУЗ СК «Ессентукский межрайонный родильный дом», Перечнем подлежащих защите персональных данных и данных, содержащих врачебную тайну, в ГБУЗ СК «Ессентукский межрайонный родильный дом» и другими локальными актами Роддома.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

**Распространение персональных данных** – действия, направленные на раскрытие ПДн неопределенному кругу, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

**Предоставление персональных данных** – действия, направленные на раскрытие ПДн определенному кругу.

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

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

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

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

**Информационная система персональных данных** – информационная система, представляющая собой совокупность содержащихся в базе данных ПДн и их обработку, информационных технологий и технических средств.

**Конфиденциальная информация** – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

**Общедоступные персональные данные** – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Трансграничная передача персональных данных** – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

#### **4. Общие условия обработки персональных данных**

4.1 Обработка ПДн в Роддоме осуществляется на основе следующих принципов:

4.1.1 Законности и справедливости обработки ПДн.

4.1.2 Законности целей и способов обработки ПДн и добросовестности.

4.1.3 Соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Роддома.

4.1.4 Соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн.

4.1.5 Достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.

4.1.6 Недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.8 Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.9 Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Роддому своих ПДн.

4.1.10 Держателем ПДн является Роддом, которому субъект ПДн передает во владение свои ПДн. Роддом выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

4.1.11 Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности

ПДн и обеспечивает безопасность информации в процессе деятельности Управления.

4.1.12 Роддом при обработке ПДн обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.

4.1.13 Мероприятия по защите ПДн определяются Положениями, приказами, инструкциями и другими внутренними документами Управления.

4.2 Для защиты ПДн в Роддоме применяются следующие принципы и правила:

4.2.1 Ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн.

4.2.2 Строгое избирательное и обоснованное распределение документов и информации между сотрудниками.

4.2.3 Рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации.

4.2.4 Знание сотрудниками требований нормативно-методических документов по защите ПДн.

4.2.5 Распределение персональной ответственности между сотрудниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн.

4.2.6 Установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных.

4.2.7 Определение угроз безопасности персональных данных при их



обработке в информационных системах персональных данных.

4.2.8 Исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника.

4.2.9 Организация порядка уничтожения персональных данных.

4.2.10 Своевременное выявление нарушений требований разрешительной системы доступа.

4.2.11 Воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

4.2.12 Регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

4.2.13 Ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.

4.2.14 Создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

4.2.15 Резервирование защищаемых данных (создание резервных копий).

4.3 Цели обработки персональных данных:

4.4.1 Исполнение требований трудового законодательства и трудового договора с сотрудником.

4.4.2 Исполнение требований законодательства в сфере охраны здоровья.

4.4.3 Ведение бухгалтерского, налогового и кадрового учета.

4.4.4 Передача персональных данных сотрудников в банковские организации для содействия в перечислении заработной платы.

4.4.5 Начисления заработной платы сотрудникам.

4.4 Правовое основание обработки персональных данных:

4.5.1 Федеральный закон Российской Федерации от 27.07.2006 №

152-ФЗ «О персональных данных».

4.5.2 Трудовой кодекс РФ.

4.5.3 Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации».

4.5.4 Федеральный закон Российской Федерации от 29.11.2010 N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации".

4.5.5 Гражданский кодекс Российской Федерации.

4.5.6 Налоговый кодекс Российской Федерации.

4.5.7 Согласие на обработку персональных данных.