*Приложение №1*

*к приказу от 29.10.2015г. № 311*

**ПОЛИТИКА**

**в отношении обработки и обеспечения безопасности персональных данных в государственном бюджетном учреждении здравоохранения Свердловской области "Рефтинская городская больница"**

**1. Общие положения**

1.1. Настоящая Политика в отношении обработки и обеспечения безопасности персональных данных в государственном бюджетном учреждении здравоохранения Свердловской области "Рефтинская городская больница" (далее соответственно — Политика, Учреждение) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ "О персональных данных" (далее — федеральный закон) в целях обеспечения защиты прав и свобод физических лиц при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также в целях соблюдения требований законодательства Российской Федерации в области персональных данных.

1.2. Настоящая Политика раскрывает основные принципы и правила, используемые Учреждением при обработке персональных данных, в том числе определяет цели, правовые основания, условия и способы такой обработки, категории субъектов персональных данных, персональные данные которых обрабатываются Учреждением, а также содержит сведения об исполнении Учреждением обязанностей в соответствии с федеральным законом и сведения о реализуемых Учреждением требованиях к защите обрабатываемых персональных данных. Политика действует в отношении всех персональных данных, обрабатываемых Учреждением.

1.3. Обеспечение безопасности персональных данных, законности и справедливости их обработки является одной из приоритетных задач Учреждения.

1.4. Политика является общедоступным документом, декларирующим концептуальные основы деятельности Учреждения при обработке персональных данных, и подлежит опубликованию на официальном сайте Учреждения в информационно-телекоммуникационной сети "Интернет" (далее — сеть интернет) по адресу [www.preft.ru](http://www.preft.ru/)

1.5. Понятия и термины, используемые в настоящей политике, применяются в значениях, установленных федеральным законом.

1.6. Настоящая Политика может быть дополнена либо изменена. Изменения в Политику вносятся по решению главного врача ГБУЗ СО "Рефтинская ГБ".

**2. Информация об операторе**

2.1. Учреждение в соответствии с федеральным законом является оператором, организующим и осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.2. Информация об операторе.

2.2.1. Полное наименование оператора: государственном бюджетном учреждении здравоохранения Свердловской области "Рефтинская городская больница".

2.2.2. Сокращённое наименование оператора: ГБУЗ СО "Рефтинская ГБ".

2.2.3. Адрес местонахождения: Свердловская область, пгт. Рефтинский, ул. Гагарина, 25.

2.2.4. Почтовый адрес оператора: 624285, Россия, Свердловская область, пгт. Рефтинский, ул. Гагарина, 25.

2.2.5. ИНН 6603007857.

2.2.6. Регистрационный номер записи в реестре операторов, осуществляющих обработку персональных данных: 11-0201990.

2.2.7. Дата внесения оператора в реестр операторов, осуществляющих обработку персональных данных / основание внесения записи в реестр: 10.06.2011г./ Приказ № 451 от 10.06.2011г.

**3. Правовые основания и цели обработки персональных данных**

3.1. Учреждение при обработке персональных данных руководствуется следующими нормативными правовыми актами:

3.1.1. Конституция Российской Федерации;

3.1.2. Трудовой кодекс Российской Федерации;

3.1.3. Налоговый кодекс Российской Федерации;

3.1.4. Федеральный закон от 01 апреля 1996 года № 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования";

3.1.5. Федеральный закон от 02 мая 2006 года № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации";

3.1.6. Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" и принятые в соответствии с ним нормативные правовые акты Российской Федерации;

3.1.7. Федеральный закон от 29 ноября 2010 года № 326-ф3 "Об обязательном медицинском страховании в Российской Федерации" и принятые в соответствии с ним нормативные правовые акты Российской Федерации;

3.1.8. Федеральный закон от 21 ноября 2011 года № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";

3.1.9. Постановление Госкомстата России от 05.01.2004 г. № 1 "Об утверждении унифицированных форм первичной учётной документации по учёту труда и его оплаты".

3.2. Учреждение обрабатывает персональные данные в следующих целях:

3.2.1. организация оказания медицинской помощи на территории городского округа Рефтинский в соответствии с законодательством Российской Федерации и законодательством Свердловской области;

3.2.2. исполнение договоров, стороной которых либо выгодоприобретателем или поручителем по которым является субъект персональных данных;

3.2.3. содействие работникам в трудоустройстве, обучение, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности, обеспечение пользования работниками установленными законодательством Российской Федерации гарантиями, компенсациями и льготами, ведение кадрового делопроизводства;

3.2.4. формирования кадрового резерва и принятие решения о трудоустройстве кандидата на замещение вакантной должности;

3.2.5. реализации права граждан на обращение в Учреждение с жалобами, заявлениями;

**4. Категории субъектов персональных данных, персональные данные которых обрабатываются Учреждением, источники их получения, сроки обработки и хранения**

4.1. Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

4.1.1. физические лица, обратившиеся за получением медицинских услуг;

4.1.2. работники Учреждения, состоящие в трудовых отношениях с Учреждением;

4.1.3. физические и юридические лица, состоящие в договорных отношениях с Учреждением;

4.1.4. близкие родственники сотрудников Учреждения;

4.1.5. граждане, обратившиеся в Учреждение с жалобами, заявлениями, их законные представители;

4.1.6. граждане, направившие резюме при устройстве на работу в Учреждение.

4.2. Источниками получения персональных данных, обрабатываемых Учреждения, являются:

4.2.1. непосредственно субъекты персональных данных (работники Учреждения, физические лица, обратившиеся за получением медицинских услуг, близкие родственники сотрудников Учреждения, граждане, обратившиеся в Учреждение, посетители, контрагенты, граждане, направившие резюме при устройстве на работу в Учреждение);

4.2.2. медицинские и страховые медицинские организации, осуществляющие деятельность на территории Свердловской области;

4.2.3. Территориальный фонд ОМС по Свердловской области;

4.2.4. Управление Пенсионного Фонда России в г. Асбесте Свердловской области;

4.2.5. Государственное учреждение - Свердловское региональное отделение Фонда социального страхования Российской Федерации;

4.2.6. Отдел ЗАГС города Асбеста Свердловской области;

4.2.7.  Министерство здравоохранения Свердловской области;

4.2.8. учреждения системы здравоохранения, подведомственные Министерству здравоохранения Свердловской области;

4.2.9. ГБУЗ СО «Рефтинская ГБ».

4.2.10. иные государственные органы и уполномоченные организации в случаях, предусмотренных законодательством Российской Федерации.

4.3. Содержание и объем обрабатываемых Учреждением персональных данных категорий субъектов персональных данных, указанных в пункте 4.1 настоящей политики, определяются в соответствии с целями обработки персональных данных, указанными в пункте 3.2 настоящей политики. Учреждение не обрабатывает персональные данные, которые являются избыточными по отношению к указанным целям обработки или несовместимы с такими целями.

4.4. В случаях, установленных пунктами 2-11 части 1 статьи 6 федерального закона, обработка Учреждением персональных данных осуществляется без согласия субъекта персональных данных на обработку его персональных данных. В иных случаях обработка Учреждением персональных данных осуществляется только с письменного согласия субъекта персональных данных на обработку его персональных данных в соответствии со статьёй 9 федерального закона.

4.5. Сроки обработки и хранения персональных данных Учреждением определяются для каждой цели обработки персональных данных в соответствии с законодательно установленными сроками хранения документации, образующейся в процессе деятельности Учреждения, в соответствии со сроком действия договора с субъектом персональных данных, сроками исковой давности, сроками хранения документов бухгалтерского учёта и на основании "Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения", утверждённого приказом Министерства культуры Российской Федерации от 25.08.2010 г. № 558, и иных требований законодательства Российской Федерации.

**5. Принципы и способы обработки персональных данных, перечень действий, совершаемых с персональными данными**

5.1. Учреждение в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 федерального закона.

5.2. Учреждение осуществляет обработку персональных данных путём сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), учёта, использования, передачи, обезличивания, блокирования, уничтожения.

5.3. В Учреждении используется смешанный (с использованием средств автоматизации и без использования средств автоматизации) способ обработки персональных данных с передачей информации по внутренней локальной сети Учреждения и с передачей информации по сети интернет в защищённом режиме.

5.4. Учреждение не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений. Обработка специальных категорий персональных данных, касающихся состояния здоровья, осуществляется Учреждением в соответствии с законодательством Российской Федерации об обязательных видах страхования, а также, в установленных случаях, по иным основаниям, указанным в части 2 статьи 10 федерального закона.

5.5. Учреждение не осуществляет обработку биометрических персональных данных субъектов персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

5.6. Учреждение не осуществляет трансграничную передачу персональных данных на территории иностранных государств.

5.7. Учреждение передаёт обрабатываемые персональные данные в уполномоченные организации, государственные органы, государственные внебюджетные фонды только на основаниях и в случаях, предусмотренных законодательством Российской Федерации, в том числе:

5.7.1. в рамках осуществления информационного взаимодействия в сфере ОМС;

5.7.2. в рамках организации оказания медицинской помощи;

5.7.3. для уплаты налогов на доходы физических лиц, обязательных страховых платежей и взносов;

5.7.4. в целях осуществления правосудия, исполнения судебного акта;

5.7.5. при ответах на официальные письменные мотивированные запросы правоохранительных органов и органов судебной власти, других уполномоченных государственных органов.

5.8. В целях информационного обеспечения в Учреждении созданы общедоступные источники персональных данных (справочники), в которые с письменного согласия работника Учреждения включаются его фамилия, имя, отчество, сведения о должности и месте работы, служебные телефонные номера и иные персонифицированные сведения, сообщаемые работником Учреждения для размещения в указанных источниках.

5.9. Учреждение прекращает обработку персональных данных в следующих случаях:

5.9.1. достижение цели обработки персональных данных;

5.9.2. изменение, признание утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;

5.9.3. выявление неправомерной обработки персональных данных, осуществляемой Учреждением;

5.9.4. отзыв субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с федеральным законом обработка персональных данных допускается только с согласия субъекта персональных данных.

5.9.5. уничтожение Учреждением персональных данных осуществляется в порядке и сроки, предусмотренные федеральным законом.

**6. Общая характеристика принимаемых Учреждением мер по обеспечению безопасности персональных данных при их обработке**

6.1. Учреждение обеспечивает конфиденциальность обрабатываемых персональных данных: не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.

6.2. Учреждение обеспечивает защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.3. Учреждение принимает необходимые правовые, организационные, технические, физические, криптографические меры защиты персональных данных, а также меры, направленные на обеспечение выполнения обязанностей, предусмотренных федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Такие меры, в том числе, включают следующие:

6.3.1. назначение работника Учреждения, ответственного за организацию обработки персональных данных;

6.3.2. издание правовых актов, регламентирующих вопросы обработки и защиты персональных данных;

6.3.3. ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, под роспись с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными актами Учреждения, регламентирующими вопросы обработки и защиты персональных данных, а также с ответственностью за разглашение персональных данных, нарушение порядка обращения с документами, содержащими такие данные, и иные неправомерные действия в отношении персональных данных;

6.3.4. создание системы внутреннего контроля соответствия обработки персональных данных законодательству Российской Федерации, в том числе требованиям к защите персональных данных;

6.3.5. анализ и оценка угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

6.3.6. реализация разрешительной системы доступа работников Учреждения и иных лиц к персональным данным и связанным с их использованием работам, материальным носителям; обеспечение соблюдения условий, при которых работники Учреждения, иные лица получают доступ к персональным данным только в пределах, необходимых для выполнения своих должностных обязанностей, либо в объёмах, вызванных необходимостью;

6.3.7. регистрация и учёт действий работников Учреждения, допущенных к персональным данным;

6.3.8. ограничение доступа работников Учреждения и иных лиц в помещения, где размещены технические средства, предназначенные для обработки персональных данных, и хранятся носители персональных данных, к информационным ресурсам, программным средствам обработки и защиты информации;

6.3.9. учёт материальных (машинных, бумажных) носителей персональных данных и обеспечение их сохранности;

6.3.10. определение мест хранения материальных носителей персональных данных и обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

6.3.11. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

6.3.12. предотвращение внедрения в информационные системы программ- вирусов, программных закладок;

6.3.13. резервирование технических средств и дублирование массивов и носителей информации;

6.3.14. обеспечение защиты персональных данных при подключении информационных систем к информационно-телекоммуникационным сетям, в том числе сети интернет;

6.3.15. обеспечение защиты персональных данных при их передаче по каналам связи, в том числе каналам связи сети интернет, с использованием средств криптографической защиты информации и электронной подписи;

6.3.16. восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

6.3.17. своевременное обнаружение фактов разглашения, утечки, несанкционированного доступа к персональным данным и принятие мер по таким фактам;

6.3.18. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем;

6.3.19. контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

6.4. Меры по обеспечению безопасности персональных данных при их обработке принимаются Учреждением с соблюдением требований федерального закона, иных нормативных правовых актов Российской Федерации, в том числе следующих:

6.4.1. постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

6.4.2. постановление Правительства Российской Федерации от 15.09.2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

6.4.3. приказ ФСТЭК России 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"; иные нормативные документы ФСТЭК России.

**7. Права субъекта персональных данных**

7.1. Субъект персональных данных имеет право на:

7.1.1 получение информации, касающейся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами, в том числе по основаниям, установленным частью 8 статьи 14 федерального закона;

7.1.2 обжалование действий или бездействия Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований федерального закона или иным образом нарушает его права и свободы;

7.1.3 защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

7.1.4 требование от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также уведомления о внесённых изменениях и предпринятых мерах третьих лиц, которым персональные данные, относящиеся к соответствующему субъекту, были переданы;

7.1.5 отзыв своего согласия на обработку персональных данных в соответствии со статьёй 9 федерального закона (в случаях, когда обработка Учреждением персональных данных осуществляется на основании согласия субъекта персональных данных).

7.2. Информация, касающаяся обработки персональных данных, предоставляется субъекту персональных данных или его представителю в доступной форме при обращении в Учреждение или при получении Учреждением запроса субъекта персональных данных или его представителя. Указанный запрос должен быть оформлен в соответствии с требованиями части 3 статьи 14 федерального закона и может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.3. Учреждение обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, предоставить безвозмездно возможность ознакомления с такими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя, а также, в установленных федеральным законом случаях, порядке и сроки, устранить нарушения законодательства Российской Федерации, допущенные при обработке персональных данных, уточнить, блокировать или уничтожить персональные данные соответствующего субъекта персональных данных.