

**Политика обработки и защиты персональных данных  
медицинской организации  
ГБУЗ «Республиканский кожно-венерологический диспансер»**

**1. Общие положения**

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом медицинской организации ГБУЗ «Республиканский кожно-венерологический диспансер» (далее – Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами, и определяемых:

– Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Министерства здравоохранения РФ от 21.11.2011 №834н «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях», оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению»
- Лицензией на оказание медицинской деятельности
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: Республика Карелия, г.Петрозаводск, ул.Фрунзе д.10. Электронная версия Политики – на сайте по адресу: <http://rkvd.karelia.ru>

## 2. Термины и принятые сокращения

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (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;

**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;

**Субъект персональных данных (Субъект)**- физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

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

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

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

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

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

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

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

**Информационная система персональных данных (ИСПД)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

**Медицинская деятельность** – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях;

**Лечащий врач** – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

### **3. Принципы обеспечения безопасности персональных данных**

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

– законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

– системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов,

условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

– комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

– непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

– своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

– минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;

– специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

## **4.Обработка персональных данных**

### **4.2. Обработка ПДн**

#### **4.2.1 Обработка персональных данных осуществляется:**

- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- с соблюдением мер, предусмотренных ст. 18.1 Федерального закона «О персональных данных».

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

Допущенные к обработке ПДн работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

#### **4.2.2 Цели обработки ПДн:**

- обеспечение населения квалифицированной дерматовенерологической помощью, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

#### **4.2.3. Категории субъектов персональных данных**

В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;

- физические лица, являющие близкими родственниками сотрудников учреждения;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

#### **4.2.4. ПДн, обрабатываемые Организацией:**

- данные полученные при осуществлении трудовых отношений;
- данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оказании дерматовенерологической помощи населению.

#### **Перечень персональных данных, обрабатываемых Организацией:**

1. Сведения о пациенте, позволяющие идентифицировать его личность (персональные данные):

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- образование, специальность;
- место работы;
- состояние в браке;
- состав семьи;
- место регистрации;
- адрес места жительства и домашний телефон;
- сведения о факте, времени, частоте обращений в медицинскую организацию;
- страховой номер индивидуального лицевого счета (СНИЛС), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
- номер полиса обязательного медицинского страхования застрахованного лица;
- данные о страховой медицинской организации, выбранной застрахованным лицом;

- дата регистрации в качестве застрахованного лица;
- статус застрахованного лица (работающий, неработающий);
- медицинская организация, оказавшая соответствующие услуги;
- виды оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объемы оказанной медицинской помощи;
- стоимость оказанной медицинской помощи;
- диагноз;
- профиль оказания медицинской помощи;
- медицинские услуги, оказанные пациенту, и примененные лекарственные препараты;
- примененные порядки и стандарты медицинской помощи;
- результат обращения за медицинской помощью;
- результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи;
- иные сведения о пациенте, позволяющие идентифицировать его личность.

2. Сведения о работнике медицинской организации, позволяющие идентифицировать его личность (персональные данные):

- фамилия, имя, отчество;
- пол;
- дата рождения;
- паспортные данные;
- СНИЛС;
- ИНН;
- место рождения;
- гражданство;
- образование, специальность;
- учёная степень;
- стаж работы;
- предыдущее место работы;
- состояние в браке;
- состав семьи;

- адрес места жительства и домашний телефон;
- сведения о заработной плате;
- сведения о номерах счетов в банках;
- сведения о воинском учете;
- заболевания, затрудняющие выполнение работником трудовых функций;
- любые иные сведения, с которыми работник считает нужным ознакомить работодателя или в предоставлении которых работодателю возникла необходимость.

#### **4.2.5. Обработка персональных данных ведется:**

- с использованием средств автоматизации.
- без использования средств автоматизации.

#### **4.3. Хранение ПДн**

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа

4.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.3.6. Хранение осуществляется в соответствии с ч.5 ст.18 Федерального закона «О персональных данных».

#### **4.4. Уничтожение ПДн**

4.4.1. При достижении целей обработки персональные данные подлежат уничтожению, если иное не предусмотрено федеральными законами.

4.4.2. Уничтожение документов, содержащих ПДн осуществляется по истечению сроков их хранения, которые регламентируются ФЗ от 21.11.1996 г. № 129-ФЗ «О бухгалтерском учете», Налоговым кодексом РФ от 31.07.1998 г. № 146-ФЗ и Приказ Минкультуры РФ от 25.08.2010 N 558 "Об утверждении "Перечня типовых управленческих архивных документов, образующихся в процессе деятельности

государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, Номенклатурой дел ГБУЗ "РКВД", утвержденной 05.05.2016

4.4.3. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.4. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.5. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

#### **4.5. Передача ПДн**

4.5.1. Передача информации, содержащей ПДн пациентов, осуществляется в организации, ведущие расчеты за оказанные медицинские услуги.

4.5.2. Передача информации, содержащее ПДн сотрудников, осуществляется в соответствии с ФЗ от 21.11.1996 г. № 129-ФЗ «О бухгалтерском учете», Налоговым кодексом РФ от 31.07.1998 г. № 146-ФЗ, Трудовым Кодексом РФ от 30.12.2001 №197-ФЗ

4.5.3. Передача предусмотрена российским в рамках установленной законодательством процедуры.

4.5.4. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- Страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- Банки для начисления заработной платы (на основании договора);
- Судебные и правоохранительные органы в случаях, установленных законодательством;

## **5. Защита персональных данных**

- 5.1. В ГБУЗ «РКВД» создаются условия и режимы защиты информации, отнесенной к ПДн, позволяющие обеспечить защиту обрабатываемых ПДн.
- 5.2. Основными мерами защиты ПДн, используемыми Организацией, являются:
- 5.2.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;
  - 5.2.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;
  - 5.2.3. Разработка политики в отношении обработки персональных данных;
  - 5.2.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД;
  - 5.2.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
  - 5.2.6. Учет машинных носителей ПДн, обеспечение их сохранности;
  - 5.2.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
  - 5.2.8. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ
  - 5.2.9. Установление правил доступа к обрабатываемым ПДн, обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
  - 5.2.10. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
  - 5.2.11. Обучение работников Организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
  - 5.2.12. Осуществление внутреннего контроля и аудита.

## 6. Основные права и обязанности

### 6.1. Основные права субъекта ПДн

Субъект ПДн имеет право:

1. на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
  - 1.1 подтверждение факта обработки персональных данных оператором;
  - 1.2 правовые основания и цели обработки персональных данных;
  - 1.3 цели и применяемые оператором способы обработки персональных данных;
  - 1.4 обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
  - 1.5 сроки обработки персональных данных, в том числе сроки их хранения;
  - 1.6 порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
  - 1.7 иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.
2. Получать сведения о наименовании и месте нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
3. Дать письменное согласие на обработку персональных данных, в т.ч. специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, если иное не установлено федеральным законом.
4. Отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

В случае отзыва субъектом персональных данных согласия на обработку персональных данных Организация вправе продолжить обработку персональных данных без согласия персональных данных при наличии оснований, указанных в Законе о персональных данных.

## **6.2. Обязанности Организации**

Организация обязана:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн в соответствии с действующим законодательства и «Правилами рассмотрения запросов субъектов персональных данных или их представителей» ГБУЗ «РКВД».
- обеспечивать хранение и обработку персональных данных, содержащихся в запросах субъектов персональных данных, с соблюдением требований российского законодательства о персональных данных.

## **7. Работа с формой обратной связи на официальном сайте ГБУЗ «РКВД»**

7.1. Официальный сайт ГБУЗ «РКВД» предоставляет возможность оставлять сообщения и задавать интересующие вопросы через форму обратной связи.

7.2. Форма обратной связи не предназначена для подачи заявления на предоставление государственных услуг.

7.3. Обращение, содержащее нецензурные либо оскорбительные выражения, угрозы жизни, здоровью и имуществу должностного лица, а также членов его семьи, может быть оставлено без ответа по существу поставленных в нём вопросов.

7.4. Информация о персональных данных граждан, направивших запрос в электронном виде, хранится и обрабатывается с соблюдением требований российского законодательства о персональных данных.