

УТВЕРЖДЕНО

Приказом ГАУЗ «РКБ им. Н.А. Семашко»  
№ 414 от «04» 06 2018 г.

## ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗУЕМЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящая Политика обработки персональных данных и реализуемых требований к защите персональных данных (далее — Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и действует в отношении всей информации, которую Государственное автономное учреждение здравоохранения «Республиканская клиническая больница им. Н.А.Семашко» Министерства здравоохранения Республики Бурятия (далее – ГАУЗ «РКБ им. Н.А. Семашко»- оператор), может получить в рамках осуществления своей деятельности. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предназначена для ознакомления неограниченного круга лиц.

В Политике определены основные цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых персональных данных, права и обязанности оператора и реализуемые требования по обеспечению безопасности персональных данных.

### ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение защиты прав и свобод субъекта персональных данных при обработке его персональных данных, безопасности объектов защиты оператора в информационных системах от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационных систем.

Политика разработана с учетом требований Конституции Российской Федерации, законодательных и иных нормативных актов Российской Федерации в области персональных данных.

Основные понятия, реализуемые в Политике:

- 1) **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2) **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;
- 3) **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;
- 4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- 5) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

8) **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;

9) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Область действия:

Требования настоящей Политики распространяются на всех работников оператора (штатных, временных, работающих по контракту и т.п.), физических лиц и их законных представителей.

## ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 1. Правовое основание обработки персональных данных

- Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ;
- Федеральный закон «Об обязательном медицинском страховании в Российской Федерации» от 29.11.2010 г. № 326-ФЗ;
- Положение о порядке обработки персональных данных работников ГАУЗ «РКБ им. Н.А. Семашко»;
- Положение о порядке обработки персональных данных работников ГАУЗ «РКБ им. Н.А. Семашко»;
- Лицензия Министерства здравоохранения Республики Бурятия на осуществление медицинской деятельности № ЛО 0301002654 от 15.08.2018 г.;
- Устав ГАУЗ «РКБ им. Н.А. Семашко»;
- Трудовой кодекс РФ;
- Гражданский кодекс РФ;
- Правила предоставления медицинскими организациями платных медицинских услуг, утвержденные Постановлением Правительства РФ от 04.10.2012 г. № 1002;
- Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
- Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»;
- Постановление Правительства РФ от 16.04.2003 № 225 «О трудовых книжках»;
- Постановление Минтруда РФ от 10.10.2003 № 69 «Об утверждении инструкции по заполнению трудовых книжек»;
- Федеральный закон от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Договоры на оказание платных медицинских услуг;
- Договоры гражданско-правового характера;
- Согласие на обработку персональных данных.

## **2. Категории субъектов персональных данных**

В ГАУЗ «РКБ им. Н.А. Семашко» обрабатываются персональные данные следующих категорий субъектов персональных данных:

- работники;
- родственники работников;
- физические лица;
- пациенты;
- родственники пациентов (законные представители);
- физические лица, обратившиеся в ГАУЗ «РКБ им. Н.А.Семашко».

## **3. Категории обрабатываемых персональных данных**

ГАУЗ «РКБ им. Н.А. Семашко» обрабатывает следующие категории персональных данных:

Работников, родственников работников, физических лиц -

фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, адрес, семейное положение, образование, профессия, доходы, состояние здоровья; пол, паспортные данные; ИНН; СНИЛС; полис ДМС (номер, организация ДМС); полис ОМС (номер, организация ОМС); сведения о воинском учете; контактная информация; информация о трудовом стаже; данные о трудовом договоре; данные об аттестации работников; данные о повышении квалификации; информация о приеме на работу, перемещении по должности, увольнении; информация об отпусках; информация о командировках; информация о больничных листах, данные документа об образовании, наименование образовательного учреждения, состав семьи, данные медицинского сертификата, фотография, данные свидетельств о заключении брака, данные свидетельств о рождении детей, данные свидетельств о расторжении брака, адрес электронной почты, данные трудовой книжки, гражданство, знание иностранных языков.

пациентов; родственников пациентов (законных представителей); физических лиц, обратившихся в ГАУЗ «РКБ им. Н.А.Семашко» -

фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; образование; профессия; состояние здоровья; состояние интимной жизни; место работы, должность, инвалидность, данные СНИЛС, данные ИНН, данные страхового медицинского полиса, паспортные данные, номер телефона, пол, адрес электронной почты.

## **4. Цели обработки персональных данных**

- оказание доврачебной, первичной, амбулаторно-поликлинической, медико-санитарной, врачебной и специализированной, высокотехнологичной медицинской помощи населению;

- обеспечение соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, организация ведения кадрового учета;

- организация ведения бухгалтерского учета, расчет, начисление и выплата заработной платы, премий и иных видов выплат.

## **5. Условия обработки, передачи и хранения персональных данных**

- ГАУЗ «РКБ им. Н.А. Семашко» при осуществлении своей деятельности в части обработки персональных данных руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

- ГАУЗ «РКБ им. Н.А. Семашко» не осуществляет трансграничную передачу персональных данных (передачу персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

- ГАУЗ «РКБ им. Н.А. Семашко» обрабатывает и хранит персональные данные субъектов в соответствии с внутренними нормативными документами, разработанными согласно законодательству Российской Федерации.

- ГАУЗ «РКБ им. Н.А. Семашко» обеспечивает конфиденциальность персональных данных в отношении всех субъектов персональных данных. Передача ПДн третьим лицам осуществляется только в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами. По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий персональные данные субъекта персональных данных без его согласия могут быть переданы в органы следствия и дознания, в органы правосудия, исполнения судебного акта, в органы надзора за соблюдением законодательства и иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

- ГАУЗ «РКБ им. Н.А. Семашко» может поручить обработку персональных данных другому лицу при выполнении следующих условий:

- получено согласие субъекта на поручение обработки персональных данных другому лицу;

- обработка персональных данных осуществляется на основании заключаемого с этим лицом договора.

Кроме того, действующее законодательство может устанавливать ограничения и другие условия, касающиеся упомянутых выше прав субъектов персональных данных.

## **6. Перечень действий с персональными данными**

ГАУЗ «РКБ им. Н.А. Семашко» осуществляет обработку (сбор; запись; систематизация; накопление; хранение; уточнение (обновление, изменение); использование; уничтожение) персональных данных без использования средств автоматизации.

ГАУЗ «РКБ им. Н.А. Семашко» может поручить обработку персональных данных третьим лицам в случаях, если:

- субъект дал согласие на осуществление таких действий (при наличии условий в договоре с третьим лицом о соблюдении им принципов и правил обработки персональных данных, предусмотренных Федеральным законом «О персональных данных»);

- для осуществления и выполнения возложенных законодательством Российской Федерации на ГАУЗ «РКБ им. Н.А. Семашко» функций, полномочий и обязанностей;

- в других случаях, предусмотренных законодательством Российской Федерации.

## **7. Трансграничная передача персональных данных не осуществляется.**

## **8. Права субъекта**

Субъект персональных данных, согласно законодательству Российской Федерации, имеет право:

- получать информацию, касающуюся обработки своих персональных данных. Для реализации вышеуказанных прав субъект персональных данных может в порядке, установленном ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обратиться к нам с соответствующим запросом. Для выполнения таких запросов представителю Оператора может потребоваться установить личность субъекта персональных данных и запросить дополнительную информацию;

- требовать уточнения своих 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;

- требовать прекращения обработки своих персональных данных в случаях, предусмотренных законодательством Российской Федерации;

- обжаловать действия или бездействие ГАУЗ «РКБ им. Н.А. Семашко» в судебном порядке;

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

## **9. Условия прекращения обработки персональных данных**

Срок или условие прекращения обработки персональных данных в ГАУЗ «РКБ им. Н.А. Семашко»:

- ликвидация ГАУЗ «РКБ им. Н.А. Семашко» или прекращение деятельности;
- истечение 75 лет – хранения персональных данных работников;
- исполнение обязательств по договорам и по истечению срока исковой давности;
- отзыв согласия если иное не предусмотрено Федеральным законодательством, либо в течение срока хранения документов согласно установленным срокам хранения для определенных категорий документов, если иное не предусмотрено Федеральным законодательством.

## **10. Принимаемые необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных граждан - субъектов персональных данных**

К мерам, применяемым ГАУЗ «РКБ им. Н.А. Семашко» для защиты персональных данных относятся:

- назначение сотрудника, ответственного за организацию обработки персональных данных;

- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону «О персональных данных»;

- разработка документов, определяющих политику ГАУЗ «РКБ им. Н.А. Семашко» в отношении обработки персональных данных, локальные документы по вопросам обработки персональных данных.

- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, с требованиями к защите персональных данных, с документами, определяющими политику ГАУЗ «РКБ им. Н.А. Семашко» в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;

- опубликование в открытом доступе, в т.ч. на официальном сайте (<http://rkbsemashko.ru>) документа, определяющего политику ГАУЗ «РКБ им. Н.А. Семашко» в отношении обработки персональных данных;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение, прошедшей в установленном порядке, процедуры оценки соответствия средств защиты информации;
- систематическое осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

## **11. Методы защиты персональных данных**

К методам защиты персональных данных относятся:

- реализация разрешительной системы допуска к обработке персональных данных;
- ограничение доступа в помещения, где хранятся носители информации;
- разграничение доступа к персональным данным;
- регистрация действий сотрудников, контроль несанкционированного доступа к персональным данным;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, использование защищенных каналов связи.

## **12. Требования по обеспечению защиты**

1. Сотрудники ГАУЗ «РКБ им. Н.А. Семашко», являющиеся пользователями информационных систем персональных данных (ИСПДн), должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

4. Сотрудники оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей, логинов и паролей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

5. Сотрудники оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

6. Сотрудники оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

9. При работе с ПДн в ИСПДн сотрудники оператора обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов.

10. При завершении работы с ИСПДн сотрудники обязаны защитить монитор с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

11. Сотрудники ГАУЗ «РКБ им. Н.А. Семашко» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили политику и процедуры безопасности ПДн.

12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

13. Ответственность сотрудников ГАУЗ «РКБ им. Н.А. Семашко»:

13.1. Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного кодекса Российской Федерации).

13.2. Сотрудники оператора несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

13.3. При нарушениях сотрудниками ГАУЗ «РКБ им. Н.А. Семашко» правил, связанных с обработкой и безопасностью ПДн, они несут ответственность дисциплинарную, административную, гражданско-правовую или уголовную ответственность, установленную действующим законодательством Российской Федерации.

### **13. Заключительные положения**

#### **1. Изменение Политики**

ГАУЗ «РКБ им. Н.А. Семашко» имеет право вносить изменения в настоящую Политику. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в общедоступном месте, если иное не предусмотрено новой редакцией Политики.

#### **2. Обратная связь**

Государственное автономное учреждение здравоохранения «Республиканская клиническая больница им. Н.А.Семашко» Министерства здравоохранения Республики Бурятия, юридический адрес: 670031, Республика Бурятия, г. Улан-Удэ, ул. Павлова, д.12, почтовый адрес: 670031, Республика Бурятия, г. Улан-Удэ, ул. Павлова, д.12.