

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 ГБУЗ «Республиканское патологоанатомическое бюро Министерства здравоохранения Республики Бурятия» (далее – ГБУЗ «РПАБ»), 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 требования к персоналу оператора, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных (ИСПДн) оператора.

ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение 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.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для субъектов ПДн. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в главе II «Правовой режим обработки персональных данных», подлежащих защите.

Область действия:

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

ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Категории субъектов персональных данных

В ГБУЗ «РПАБ» обрабатываются персональные данные следующих категорий субъектов персональных данных:

- служащих и работников (лиц, состоящих в трудовых отношениях с ГБУЗ «РПАБ»);
- пациентов, поступившие в медицинской документации из различных лечебно-профилактических учреждений для проведения патологоанатомических исследований, охватывающих прижизненную и посмертную диагностику заболеваний.

2. Категории обрабатываемых персональных данных

ГБУЗ «РПАБ» обрабатывает следующие категории персональных данных:

2.1. Персональные данные: фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, данные паспорта, семейное положение, социальное положение,

имущественное положение, образование, профессия, доходы, сведения о составе семьи; сведения о социальных льготах индивидуальный номер налогоплательщика (ИНН); номер страхового свидетельства (СНИЛС); реквизиты полиса ОМС (ДМС) контактный телефон другая информация, относящаяся к субъекту персональных данных.

2.2. Специальные категории персональных данных: состояние здоровья.

2.3. Биометрические персональные данные: пол, рост, вес, группа крови, резус принадлежность.

3. Цели обработки персональных данных

3.1. Исполнение положений нормативных правовых актов.

3.2. Работники: содействие в трудовой деятельности, обеспечение личной безопасности, учет результатов исполнения договорных обязательств, осуществление безналичных платежей на счет работника, обеспечение работоспособности и сохранности ресурсов и имущества работодателя, осуществление коллективного взаимодействия и совместного использования информационных ресурсов, аттестация, повышение квалификации, а также наиболее полное исполнение обязательств и компетенций в соответствии с Трудовым кодексом Российской Федерации, и другими нормативно-правовыми актами Российской Федерации в сфере трудовых отношений.

3.3. Пациенты, родители, законные представители: с целью исполнения требований законодательства РФ (Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья в Российской Федерации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и других нормативно-правовых актов Российской Федерации); с целью исполнения договорных отношений.

4. Условия обработки, передачи и хранения персональных данных

4.1. ГБУЗ «РПАБ», при осуществлении своей деятельности в части обработки персональных данных руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

4.2. ГБУЗ «РПАБ» не осуществляет трансграничную передачу персональных данных (передачу персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

4.3. ГБУЗ «РПАБ» обрабатывает и хранит персональные данные субъектов в соответствии с внутренними нормативными документами, разработанными согласно законодательству РФ.

4.4. ГБУЗ «РПАБ» обеспечивает конфиденциальность персональных данных в отношении всех субъектов персональных данных. Передача ПДн третьим лицам осуществляется только при выполнении функции предоставления медицинских услуг - в рамках установленной законодательством процедуры.

4.5. Оператор 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.

5. Перечень действий с персональными данными

ГБУЗ «РПАБ» осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных с использованием средств автоматизации, а также без использования таких средств.

ГБУЗ «РПАБ» 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 ГБУЗ «РПАБ» функций, полномочий и обязанностей;

- в других случаях, предусмотренных законодательством Российской Федерации.

Трансграничная передача персональных данных не осуществляется.

6. Права субъекта

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

- получать информацию, касающуюся обработки своих персональных данных;

- 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 ГБУЗ «РПАБ» в судебном порядке;

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

7. Условия прекращения обработки персональных данных

Срок или условие прекращения обработки персональных данных в ГБУЗ «РПАБ»:

- ликвидация ГБУЗ «РПАБ» или прекращение деятельности;

- истечение 75 лет хранения персональных данных работников;

- исполнение обязательств по договорам и в течение 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.

8. ГБУЗ «РПАБ» принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных граждан - субъектов персональных данных

К мерам, применяемым 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, определяющие политику ГБУЗ «РПАБ» в отношении обработки персональных данных, локальные документы по вопросам обработки персональных данных.

- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, с требованиями к защите персональных данных, с документами, определяющими политику ГБУЗ «РПАБ» в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;

- опубликование в сети Интернет документа, определяющего политику ГБУЗ «РПАБ» 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.

9. Методы защиты персональных данных

К методам защиты персональных данных относятся:

- реализация разрешительной системы допуска к обработке персональных данных;
- ограничение доступа в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также 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.

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ

1. Сотрудники ГБУЗ «РПАБ», 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 ГБУЗ «РПАБ» 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 ГБУЗ «РПАБ»:

13.1. Действующее законодательство РФ 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 ГБУЗ «РПАБ» правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1. Изменение Политики

ГБУЗ «РПАБ» 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 бюджетное учреждение здравоохранения «Республиканское патологоанатомическое бюро Министерства здравоохранения Республики Бурятия», юридический адрес: 670031, Республика Бурятия, г. Улан-Удэ, ул. Павлова, д. 12.