



МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ ПЕРМСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
ПЕРМСКОГО КРАЯ
«ГОРНОЗАВОДСКАЯ РАЙОННАЯ БОЛЬНИЦА»



УТВЕРЖДАЮ
Главный врач
Роман Владимир Тарасович
2026 г.

Приложение №1
к приказу № 181 от 16.08.2026 г.

ПОЛОЖЕНИЕ

в отношении обработки и защиты персональных данных
в Государственном бюджетном учреждении здравоохранения Пермского края
«Горнозаводская районная больница»

1. Общие положения

1.1. Настоящая Политика в отношении обработки и защиты персональных данных в Государственном бюджетном учреждении здравоохранения Пермского края «Горнозаводская районная больница» (далее — Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, категории субъектов персональных данных и обрабатываемых персональных данных, права субъектов персональных данных, обязанности Оператора, а также основные меры, принимаемые Оператором для обеспечения безопасности персональных данных.

1.2. Оператором персональных данных является:

полное наименование: Государственное бюджетное учреждение здравоохранения Пермского края «Горнозаводская районная больница»;

сокращенное наименование: ГБУЗ ПК «Горнозаводская РБ»;

ОГРН: 1155958058464;

ИНН: 5921032100;

КПП: 592101001;

адрес: 618820, Пермский край, Горнозаводский район, г. Горнозаводск, ул. Свердлова, д. 73;

официальный сайт: <https://gorno-zrb.ru/>;

адрес электронной почты: info-gornrb@med.permkrai.ru.

Далее ГБУЗ ПК «Горнозаводская РБ» именуется также Учреждением или Оператором.

1.3. Политика разработана в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Трудовым кодексом Российской Федерации, Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», постановлением Правительства Российской Федерации от 15.09.2008 № 687, постановлением Правительства Российской Федерации от 01.11.2012 № 1119 и иными нормативными правовыми актами Российской Федерации, регулирующими вопросы обработки и защиты персональных данных.

1.4. Политика разработана во исполнение требований статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, а применительно к пациентам — также сведений, составляющих врачебную тайну.

1.5. Действие Политики распространяется на обработку персональных данных, осуществляемую Оператором как с использованием средств автоматизации, так и без использования таких средств.

1.6. Требования Политики обязательны для работников Оператора, имеющих доступ к персональным данным или осуществляющих их обработку.

1.7. Оператор обеспечивает неограниченный доступ к настоящей Политике. Актуальная редакция Политики размещается на официальном сайте Оператора <https://gorno-zrb.ru/>, в том числе обеспечивается возможность доступа к ней со страниц сайта, посредством которых осуществляется сбор персональных данных.

2. Основные понятия

2.1. Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу — субъекту персональных данных.

2.2. 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 и действия, совершаемые с ними.

2.3. Обработка персональных данных — любое действие или совокупность действий, совершаемых с персональными данными с использованием средств автоматизации или без их использования, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, распространение, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение.

2.4. Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

2.5. Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.6. Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.7. Блокирование персональных данных — временное прекращение обработки персональных данных, за исключением случаев, когда обработка необходима для их уточнения.

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

2.9. Обезличивание персональных данных — действия, в результате которых без использования дополнительной информации становится невозможным определить принадлежность персональных данных конкретному субъекту.

2.10. Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.11. Персональные данные, разрешенные субъектом персональных данных для распространения, — персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом путем дачи соответствующего согласия в порядке, предусмотренном законодательством Российской Федерации.

2.12. Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных Оператором осуществляется на законной и справедливой основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей.

3.3. Не допускается обработка персональных данных, несовместимая с целями их сбора.

3.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых целях.

3.5. Обработке подлежат только персональные данные, соответствующие целям их обработки.

3.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Не допускается обработка избыточных персональных данных.

3.7. Оператор обеспечивает точность, достаточность и при необходимости актуальность персональных данных и принимает меры по уточнению или удалению неполных, устаревших или неточных данных.

3.8. Персональные данные хранятся в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки, если срок хранения не установлен законодательством Российской Федерации, договором или иным законным основанием.

3.9. По достижении целей обработки или в случае утраты необходимости в их достижении персональные данные уничтожаются либо обезличиваются, если иное не предусмотрено законодательством Российской Федерации.

3.10. Доступ работников Оператора к персональным данным предоставляется только в объеме, необходимом для исполнения их должностных обязанностей.

4. Цели обработки персональных данных

4.1. Оператор осуществляет обработку персональных данных в целях:

оказания медицинской помощи населению;

ведения медицинской документации;

организации профилактических мероприятий, диспансеризации, медицинских осмотров и иных предусмотренных законодательством мероприятий;

выполнения обязанностей медицинской организации в системе обязательного медицинского страхования;

передачи предусмотренных законодательством сведений в государственные информационные системы в сфере здравоохранения;

обеспечения лекарственного обеспечения и осуществления фармацевтической деятельности;

ведения кадрового, бухгалтерского, налогового и воинского учета;

заключения, исполнения и прекращения трудовых договоров;

начисления и выплаты заработной платы и иных выплат;

исчисления и уплаты налогов, страховых взносов и иных обязательных платежей;

представления обязательной отчетности в государственные органы и государственные внебюджетные фонды;

подбора кандидатов на замещение вакантных должностей;

заключения и исполнения гражданско-правовых договоров;

рассмотрения обращений, заявлений, запросов и жалоб граждан;

организации пропускного и внутриобъектового режима в предусмотренных случаях;

обеспечения безопасности пациентов, посетителей, работников и имущества Оператора;

обеспечения антитеррористической защищенности объектов Оператора;

осуществления видеонаблюдения;

обеспечения функционирования официального сайта и обработки обращений, поступающих посредством сайта;

выполнения иных функций, полномочий и обязанностей, возложенных на Оператора законодательством Российской Федерации.

5. Категории субъектов персональных данных

5.1. Оператор обрабатывает персональные данные следующих категорий субъектов:

пациенты, в том числе несовершеннолетние;

законные представители пациентов;

родственники пациентов и иные лица, сведения о которых законно включаются в медицинскую документацию;

работники Оператора;

бывшие работники;

члены семей и родственники работников в случаях, предусмотренных законодательством;

кандидаты на замещение вакантных должностей;

физические лица, заключившие с Оператором гражданско-правовые договоры;

представители, работники и иные физические лица контрагентов;

лица, направляющие Оператору обращения, заявления, запросы или жалобы;

посетители объектов Оператора;

пользователи официального сайта;

иные физические лица, персональные данные которых Оператор обязан или вправе обрабатывать в соответствии с законодательством Российской Федерации.

6. Категории обрабатываемых персональных данных

6.1. В зависимости от конкретной цели Оператор может обрабатывать:

фамилию, имя, отчество;

пол;

дату и место рождения;

гражданство;

адрес регистрации и адрес фактического проживания;

контактные данные, включая номера телефонов и адрес электронной почты;

сведения документов, удостоверяющих личность;

СНИЛС;

ИНН;

сведения полиса обязательного или добровольного медицинского страхования;

сведения об образовании, специальности, квалификации и профессиональной подготовке;

сведения о трудовой деятельности;

сведения о воинском учете;

банковские реквизиты;

сведения о доходах, начислениях и удержаниях;

сведения о членах семьи и родственниках в предусмотренных законом случаях;

сведения, необходимые для исполнения гражданско-правовых договоров;

сведения, содержащиеся в обращениях и заявлениях;

фото- и видеоизображения в случаях осуществления видеонаблюдения;

иные персональные данные, обработка которых необходима для достижения конкретной законной цели.

6.2. В связи с осуществлением медицинской деятельности Оператор обрабатывает специальные категории персональных данных, касающиеся состояния здоровья субъектов, в том числе сведения о заболеваниях, диагнозах, результатах обследований, медицинских вмешательствах, лечении, состоянии здоровья и иные сведения медицинского характера.

6.3. Объем обрабатываемых персональных данных определяется исходя из соответствующей цели и не должен быть избыточным.

7. Правовые основания обработки персональных данных

7.1. Правовыми основаниями обработки персональных данных являются нормативные правовые акты Российской Федерации, регулирующие деятельность Оператора, а также:

согласие субъекта персональных данных в случаях, когда его получение необходимо;

необходимость исполнения функций, полномочий и обязанностей, возложенных на Оператора законодательством;

необходимость исполнения договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, либо заключения договора по инициативе субъекта;

необходимость защиты жизни, здоровья или иных жизненно важных интересов субъекта или других лиц, если получение согласия невозможно;

иные основания, предусмотренные Федеральным законом № 152-ФЗ и другими федеральными законами.

7.2. В случаях, когда законодательство Российской Федерации предоставляет Оператору право осуществлять обработку персональных данных без согласия субъекта, получение отдельного согласия не является обязательным.

8. Согласие субъекта персональных данных

8.1. Если правовым основанием обработки является согласие субъекта, оно должно быть конкретным, предметным, информированным, сознательным и однозначным.

8.2. Согласие на обработку персональных данных оформляется отдельно от иных информации и (или) документов, которые подтверждает или подписывает субъект персональных данных.

8.3. Согласие должно распространяться только на персональные данные и действия, необходимые для заявленной цели обработки.

8.4. Субъект вправе отозвать согласие.

8.5. После отзыва согласия Оператор вправе продолжить обработку персональных данных только при наличии другого предусмотренного законом основания.

8.6. Обязанность подтвердить получение согласия либо наличие иного законного основания для обработки персональных данных возлагается на Оператора.

9. Специальные категории персональных данных

9.1. В связи с медицинской деятельностью Оператор осуществляет обработку сведений о состоянии здоровья пациентов.

9.2. Обработка указанных сведений производится в случаях и на основаниях, предусмотренных законодательством Российской Федерации, в том числе в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинской и медико-социальной помощи лицами, обязанными сохранять врачебную тайну.

9.3. Доступ к медицинской информации предоставляется работникам только в пределах их должностных полномочий.

9.4. Обработка иных специальных категорий персональных данных допускается только при наличии предусмотренного законом основания.

10. Биометрические персональные данные и видеонаблюдение

10.1. Оператор не осуществляет обработку биометрических персональных данных в целях установления личности субъекта с использованием систем распознавания лиц, отпечатков пальцев или иных технологий биометрической идентификации, за исключением случаев, если такая обработка будет введена в будущем на предусмотренном законодательством основании.

10.2. На отдельных объектах Оператора осуществляется видеонаблюдение.

10.3. Целями видеонаблюдения являются обеспечение безопасности пациентов, посетителей и работников, сохранности имущества, обеспечение внутриобъектового режима и антитеррористической защищенности объектов.

10.4. Видеонаблюдение не используется для автоматизированного распознавания лиц и установления личности субъектов на основании их физиологических или биологических особенностей.

10.5. Видеонаблюдение осуществляется с учетом необходимости соблюдения права граждан на неприкосновенность частной жизни.

10.6. Камеры не размещаются в местах, где видеонаблюдение очевидно нарушало бы право граждан на частную жизнь, за исключением прямо предусмотренных законодательством случаев.

10.7. Доступ к видеозаписям предоставляется ограниченному кругу уполномоченных работников.

10.8. Сроки хранения видеозаписей устанавливаются локальными нормативными актами Оператора исходя из целей видеонаблюдения и требований законодательства. По истечении установленного срока записи удаляются либо перезаписываются, если отсутствует законное основание для их дальнейшего хранения.

11. Способы обработки и информационные системы

11.1. Оператор осуществляет:

автоматизированную обработку персональных данных;

неавтоматизированную обработку персональных данных;

смешанную обработку персональных данных.

11.2. Автоматизированная обработка осуществляется с применением информационных систем и программного обеспечения, используемых Оператором при выполнении возложенных на него функций.

11.3. К таким системам относятся, в частности:

медицинская информационная система;

лабораторная информационная система при ее использовании;

программные продукты семейства «1С», используемые для бухгалтерского, кадрового учета и расчета заработной платы;

Единая государственная информационная система в сфере здравоохранения и иные федеральные и региональные государственные информационные системы, к которым Оператор имеет предоставленный в установленном порядке доступ;

специализированное программное обеспечение медицинского оборудования, в том числе рентгенодиагностического оборудования, если посредством него

осуществляется обработка сведений, относящихся к определенным или определяемым пациентам;

иные информационные системы, необходимые для выполнения функций Оператора.

11.4. Наличие у информационной системы иного владельца, обладателя или администратора не освобождает Оператора от выполнения установленных законодательством обязанностей применительно к персональным данным, которые Оператор собирает, вводит, использует, получает или передает посредством такой системы в рамках собственной деятельности.

11.5. Объем обязанностей Оператора и владельца, обладателя, администратора либо иного участника функционирования внешней информационной системы определяется законодательством Российской Федерации, нормативными правовыми актами, регламентами соответствующей системы, соглашениями и договорами.

11.6. Перечень конкретных информационных систем, программного обеспечения, рабочих мест, серверов, баз данных и технических средств, используемых для обработки персональных данных, ведется во внутренних документах Оператора и не подлежит обязательному опубликованию в составе настоящей Политики.

12. Сбор персональных данных и локализация баз данных

12.1. Персональные данные преимущественно получают непосредственно от субъекта персональных данных либо его законного представителя.

12.2. Получение персональных данных от третьих лиц допускается при наличии предусмотренного законодательством основания.

12.3. Если персональные данные получены не от субъекта, Оператор выполняет обязанности по информированию субъекта в случаях, предусмотренных Федеральным законом № 152-ФЗ.

12.4. При сборе персональных данных граждан Российской Федерации, в том числе посредством информационно-телекоммуникационной сети Интернет, запись, систематизация, накопление, хранение, уточнение и извлечение таких данных осуществляются с использованием баз данных, находящихся на территории Российской Федерации, за исключением прямо установленных законодательством случаев.

12.5. При использовании официального сайта Оператор организует сбор персональных данных таким образом, чтобы объем собираемых сведений соответствовал цели обращения пользователя.

13. Обработка персональных данных на официальном сайте

13.1. Официальным сайтом Оператора является <https://gorno-zrb.ru/>.

13.2. При использовании размещенных на сайте форм обращений и иных сервисов могут обрабатываться сведения, непосредственно предоставленные пользователем.

13.3. До направления пользователем сведений посредством формы сбора персональных данных ему должна быть обеспечена возможность ознакомиться с настоящей Политикой и иной необходимой информацией об обработке персональных данных.

13.4. Оператор не использует иностранные интернет-сервисы и иностранные облачные сервисы для обработки персональных данных посредством официального сайта.

13.5. Подключение к официальному сайту сторонних аналитических, статистических, облачных и иных сервисов, получающих доступ к персональным данным пользователей, допускается только после предварительной оценки законности их использования, местонахождения используемых баз данных и наличия либо отсутствия трансграничной передачи персональных данных.

14. Передача персональных данных третьим лицам

14.1. Оператор обеспечивает конфиденциальность персональных данных и не раскрывает их третьим лицам без согласия субъекта, если иное не предусмотрено федеральным законом.

14.2. Персональные данные могут предоставляться в установленном законодательством порядке:

государственным органам;

органам государственных внебюджетных фондов;

налоговым органам;

органам обязательного медицинского страхования;

страховым медицинским организациям;

органам управления здравоохранением;

судам;

правоохранительным органам;

кредитным организациям в необходимых случаях;

организациям, обеспечивающим функционирование информационных систем, при наличии соответствующего законного основания;

иным получателям, если предоставление предусмотрено законодательством или осуществляется с согласия субъекта.

14.3. Передаваемый объем персональных данных ограничивается сведениями, необходимыми для достижения соответствующей законной цели.

15. Поручение обработки персональных данных другому лицу

15.1. Оператор вправе поручить обработку персональных данных другому лицу на основании договора, государственного контракта или иного предусмотренного законом документа.

15.2. В поручении Оператор определяет перечень персональных данных, перечень действий с ними, цели обработки и устанавливает обязанность лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных.

15.3. Поручение должно также предусматривать выполнение требований законодательства о защите персональных данных, предоставление Оператору документов и сведений, подтверждающих выполнение установленных требований, и обязанность сообщать Оператору об инцидентах с персональными данными.

15.4. Оператор осуществляет контроль за соблюдением условий поручения в пределах, установленных законодательством и договором.

16. Трансграничная передача персональных данных

16.1. На дату утверждения настоящей Политики Оператор **не осуществляет трансграничную передачу персональных данных.**

16.2. Оператор не использует иностранные облачные или иные иностранные сервисы для хранения и обработки персональных данных.

16.3. В случае возникновения необходимости осуществления трансграничной передачи Оператор до ее начала обеспечивает выполнение требований статьи 12

Федерального закона № 152-ФЗ, включая получение предусмотренной законом информации о получателе персональных данных и направление отдельного уведомления в уполномоченный орган по защите прав субъектов персональных данных.

16.4. До выполнения установленных законом условий трансграничная передача персональных данных Оператором не осуществляется.

17. Хранение персональных данных

17.1. Персональные данные хранятся только в течение сроков, необходимых для достижения целей обработки, если иной срок не установлен законодательством Российской Федерации, договором или иным законным основанием.

17.2. Конкретные сроки хранения документов устанавливаются законодательством Российской Федерации об архивном деле, отраслевыми требованиями, номенклатурой дел Оператора и иными локальными нормативными актами.

17.3. Бумажные носители персональных данных хранятся в помещениях и местах, исключающих доступ неуполномоченных лиц.

17.4. Доступ к электронным персональным данным разграничивается с учетом должностных обязанностей работников.

17.5. Не допускается размещение персональных данных в общедоступных сетевых каталогах, файлообменниках, несанкционированных облачных хранилищах и иных ресурсах, не предусмотренных установленным Оператором порядком обработки персональных данных.

18. Уничтожение персональных данных

18.1. Персональные данные уничтожаются либо обезличиваются при достижении целей обработки или утрате необходимости в их достижении, если иное не предусмотрено законодательством.

18.2. Бумажные документы уничтожаются способом, исключающим возможность восстановления содержащейся в них информации.

18.3. Персональные данные в электронном виде уничтожаются средствами и способами, исключающими возможность их дальнейшего восстановления в случаях, установленных законодательством.

18.4. Подтверждение уничтожения персональных данных осуществляется в соответствии с требованиями уполномоченного органа по защите прав субъектов персональных данных и локальными документами Оператора.

18.5. При отсутствии возможности уничтожения персональных данных в установленный срок Оператор осуществляет их блокирование и обеспечивает уничтожение в срок, предусмотренный законодательством Российской Федерации.

19. Права субъектов персональных данных

19.1. Субъект персональных данных имеет право получать информацию, касающуюся обработки его персональных данных, в объеме, установленном Федеральным законом № 152-ФЗ.

19.2. Субъект вправе требовать уточнения, блокирования или уничтожения своих персональных данных, если они являются неполными, устаревшими, неточными, незаконно полученными либо не являются необходимыми для заявленной цели обработки.

19.3. Субъект вправе отозвать согласие на обработку персональных данных, если обработка осуществляется на основании согласия.

19.4. Субъект вправе потребовать прекращения обработки его персональных данных в предусмотренных законом случаях.

19.5. Субъект имеет право получить информацию об осуществленной либо предполагаемой трансграничной передаче персональных данных.

19.6. Субъект вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных либо непосредственно в судебном порядке.

20. Порядок рассмотрения обращений субъектов персональных данных

20.1. Субъект персональных данных или его представитель вправе направить обращение:

по адресу: 618820, Пермский край, Горнозаводский район, г. Горнозаводск, ул. Свердлова, д. 73;

по электронной почте: info-gornrb@med.permkrai.ru;

посредством предусмотренных официальным сайтом каналов связи.

20.2. Информация о наличии и обработке персональных данных предоставляется субъекту или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса.

20.3. Указанный срок может быть продлен не более чем на 5 рабочих дней при направлении субъекту мотивированного уведомления с указанием причин продления.

20.4. В случае отказа в предоставлении информации Оператор направляет мотивированный ответ в сроки, установленные законодательством.

20.5. При подтверждении того, что персональные данные являются неполными, неточными или неактуальными, Оператор вносит необходимые изменения в срок не более 7 рабочих дней.

20.6. Если подтверждено, что персональные данные незаконно получены или не требуются для заявленной цели, Оператор уничтожает их в срок не более 7 рабочих дней.

20.7. При получении требования о прекращении обработки персональных данных Оператор прекращает обработку в срок не более 10 рабочих дней, за исключением случаев, когда законодательство предоставляет право продолжить такую обработку.

20.8. Срок, предусмотренный пунктом 20.7 настоящей Политики, может быть продлен не более чем на 5 рабочих дней с направлением субъекту мотивированного уведомления.

21. Действия при выявлении нарушений обработки персональных данных

21.1. При выявлении неправомерной обработки персональных данных Оператор осуществляет блокирование соответствующих данных либо обеспечивает их блокирование на период проверки.

21.2. При выявлении неточных данных они блокируются на период проверки, если такое блокирование не нарушает права и законные интересы субъекта или третьих лиц.

21.3. При подтверждении неточности персональные данные уточняются в течение 7 рабочих дней.

21.4. При выявлении неправомерной обработки Оператор прекращает неправомерную обработку либо обеспечивает ее прекращение в срок не более 3 рабочих дней со дня выявления нарушения.

21.5. Если обеспечить правомерность обработки невозможно, персональные данные уничтожаются в срок не более 10 рабочих дней с даты выявления неправомерной обработки.

21.6. При достижении цели обработки Оператор прекращает обработку и уничтожает персональные данные в срок не более 30 дней, если законодательством, договором или иным законным основанием не предусмотрено дальнейшее хранение или обработка.

21.7. При отзыве согласия на обработку персональных данных и отсутствии иных законных оснований для их обработки Оператор обеспечивает прекращение обработки и уничтожение персональных данных в срок не более 30 дней.

22. Действия при инцидентах с персональными данными

22.1. Оператор организует выявление, учет, внутреннее расследование и устранение последствий инцидентов, связанных с неправомерным или случайным доступом, предоставлением, распространением или иной передачей персональных данных.

22.2. При установлении факта неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор уведомляет уполномоченный орган по защите прав субъектов персональных данных:

в течение 24 часов с момента выявления инцидента — о произошедшем инциденте, его предполагаемых причинах, предполагаемой вреде, принятых мерах и лице, уполномоченном на взаимодействие с уполномоченным органом;

в течение 72 часов — о результатах внутреннего расследования и о лицах, действия которых стали причиной инцидента, при наличии таких сведений.

22.3. Оператор обеспечивает в предусмотренном законодательством порядке взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

22.4. Работник, выявивший либо предполагающий наличие инцидента, обязан незамедлительно сообщить об этом лицу, ответственному за организацию обработки персональных данных, и работнику, ответственному за защиту информации, в соответствии с локальным порядком реагирования.

23. Меры по защите персональных данных

23.1. Оператор принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

23.2. В числе таких мер Оператор осуществляет:

- назначение лица, ответственного за организацию обработки персональных данных;
- назначение лиц, ответственных за обеспечение безопасности персональных данных и защиту информации, в пределах установленной организационной структуры;
- разработку и актуализацию локальных нормативных актов;
- определение целей обработки и перечней обрабатываемых персональных данных;
- определение актуальных угроз безопасности персональных данных;
- установление правил доступа к персональным данным;
- разграничение прав пользователей информационных систем;
- идентификацию и аутентификацию пользователей;
- учет машинных носителей информации;
- регистрацию и учет предусмотренных действий пользователей;
- применение антивирусной защиты, межсетевого экранирования и иных средств защиты информации;
- обнаружение фактов несанкционированного доступа;
- резервное копирование и восстановление информации;
- принятие мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак;
- оценку эффективности принимаемых мер;
- внутренний контроль и (или) аудит;
- оценку вреда, который может быть причинен субъектам персональных данных;
- ознакомление работников с законодательством и локальными нормативными актами;

обучение и инструктаж работников, непосредственно участвующих в обработке персональных данных.

23.3. Конкретный состав применяемых средств защиты, программного обеспечения, сетевого оборудования, адресов технических средств, версий программ и иных технических сведений определяется внутренними документами Оператора и в настоящей публичной Политике не раскрывается.

24. Лицо, ответственное за организацию обработки персональных данных

24.1. Ответственный за организацию обработки персональных данных назначается приказом главного врача Оператора.

24.2. Ответственный получает указания непосредственно от исполнительного органа Оператора и подотчетен ему.

24.3. Ответственный осуществляет внутренний контроль за соблюдением законодательства о персональных данных, доводит требования законодательства и локальных документов до работников, организует прием и обработку обращений субъектов персональных данных и выполняет иные возложенные на него обязанности.

24.4. Ответственные за техническую защиту информации и обеспечение безопасности отдельных информационных систем могут назначаться отдельными приказами Оператора.

25. Внутренний контроль

25.1. Оператор осуществляет внутренний контроль соответствия обработки персональных данных требованиям законодательства Российской Федерации и локальных нормативных актов.

25.2. Контролю подлежат в том числе обработка персональных данных в информационных системах, неавтоматизированная обработка, официальный сайт, видеонаблюдение, формы согласий, договоры с третьими лицами, соблюдение сроков хранения и уничтожения, рассмотрение обращений и порядок реагирования на инциденты.

25.3. Перечень информационных систем и программных средств подлежит периодической актуализации.

25.4. Специализированное программное обеспечение медицинского оборудования подлежит включению в учет информационных ресурсов в случае, если в нем осуществляется хранение или иная обработка сведений, позволяющих определить конкретного пациента.

26. Конфиденциальность персональных данных

26.1. Оператор, его работники и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта, если иное не предусмотрено федеральным законом.

26.2. Доступ к персональным данным предоставляется только работникам, которым такой доступ необходим для исполнения должностных обязанностей.

26.3. Работники, непосредственно осуществляющие обработку персональных данных, знакомятся с нормативными требованиями и локальными документами Оператора.

27. Ответственность

27.1. Лица, виновные в нарушении требований законодательства Российской Федерации в области персональных данных и локальных нормативных актов Оператора, несут предусмотренную законодательством дисциплинарную, материальную, гражданско-правовую, административную, уголовную и иную ответственность.

27.2. Оператор несет ответственность за выполнение возложенных на него законодательством обязанностей независимо от использования информационных систем, владельцами или администраторами которых являются иные организации, в пределах функций и операций с персональными данными, осуществляемых Оператором.

27.3. Положения настоящей Политики не могут толковаться как ограничивающие предусмотренные законодательством права субъектов персональных данных или освобождающие Оператора от установленной законом ответственности.

28. Заключительные положения

28.1. Настоящая Политика вступает в силу с даты ее утверждения приказом главного врача ГБУЗ ПК «Горнозаводская РБ».

28.2. С даты вступления настоящей Политики в силу ранее действовавшая Политика обработки и защиты персональных данных ГБУЗ ПК «Горнозаводская РБ», утвержденная в 2017 году, признается утратившей силу.

28.3. Политика пересматривается при изменении законодательства Российской Федерации, целей или способов обработки персональных данных, состава информационных систем, порядка использования официального сайта, организации видеонаблюдения либо иных обстоятельств, влияющих на обработку и защиту персональных данных.

28.4. Оператор обеспечивает размещение актуальной редакции Политики на официальном сайте <https://gorno-zrb.ru/>.

28.5. Контроль за актуальностью настоящей Политики осуществляет лицо, ответственное за организацию обработки персональных данных.

28.6. Контактные данные для обращений по вопросам обработки персональных данных:

ГБУЗ ПК «Горнозаводская РБ»

618820, Пермский край, Горнозаводский район,
г. Горнозаводск, ул. Свердлова, д. 73.

Электронная почта: info-gornrb@med.permkrai.ru

Официальный сайт: <https://gorno-zrb.ru/>