

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ ХАКАСИЯ
«КОПЬЁВСКАЯ РАЙОННАЯ БОЛЬНИЦА»
(ГБУЗ РХ «Копьёвская РБ»)**

П Р И К А З

« 26 » апреля 2021 г.

№ 131

п. Копьево

**Об утверждении Политики в отношении обработки
и защиты персональных данных**

В соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», в целях обеспечения защиты прав и свобод человека и гражданина при обработке персональных данных в ГБУЗ РХ «Копьёвская РБ», приказываю:

1. Утвердить Политику в отношении обработки и защиты персональных данных (Приложение №1).
2. Администратору информационной безопасности Кривошееву О.В. обеспечить неограниченный доступ к настоящему приказу путем его опубликования на странице учреждения официального интернет-портала Министерства здравоохранения Республике Хакасия.
3. Контроль исполнения приказа оставляю за собой.

Главный врач
ГБУЗ РХ «Копьёвская РБ»



В.Н. Кулымова

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая Политика в отношении обработки и защиты персональных данных (далее – Политика) составлена в соответствии с Федеральным законом №152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим документом ГБУЗ РХ «Копьёвская РБ» (далее – медучреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных, оператором которых является медучреждение.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в медучреждении, 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 персональных данных, полученных медучреждением 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 персональных данных, полученных до ее утверждения.

1.4. Обработка и защита персональных данных в медучреждении осуществляется в связи с выполнением медучреждением функций, предусмотренных ее учредительными документами, и в соответствии с:

- Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- 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»;
- иными нормативными правовыми актами Российской Федерации.

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

1.5. Медучреждение имеет право вносить изменения в «Политику в отношении обработки и защиты персональных данных».

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 медучреждения по адресу: Республика Хакасия, Орджоникидзевский район, п.Копьево, ул. Зеленая 50.
Электронная версия Политики на сайте по адресу: <http://kopcrb.ru>

2. Термины и принятые сокращения

Персональные данные - 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.

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.

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. Задачи и принципы обеспечения безопасности персональных данных

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

3.2. Для обеспечения безопасности персональных данных медучреждение руководствуется следующими принципами:

- законность: защита персональных данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты персональных данных. Обработка персональных данных должна осуществляться на законной и справедливой основе. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- системность: обработка персональных данных осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных;

- комплексность: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах медучреждения и других имеющихся в учреждении систем и средств защиты;

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

- своевременность: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки;

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

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

- минимизация прав доступа: доступ к персональным данным предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

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

– специализация и профессионализм: реализация мер по обеспечению безопасности персональных данных осуществляется Работниками, имеющими необходимые квалификацию и опыт;

– эффективность процедур отбора кадров: кадровая политика медучреждения предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности персональных данных;

– наблюдаемость и прозрачность: меры по обеспечению безопасности персональных данных должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

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

3.3. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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

3.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Медучреждение должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

4. Организация работы с персональными данными

4.1. Получение персональных данных.

4.1.1. Все персональные данные следует получать от самого субъекта. Если персональные данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Медучреждение должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие персональные данные, создаются путем:

- а) копирования оригиналов документов;
- б) внесения сведений в учетные формы;
- в) получения оригиналов необходимых документов.

Порядок доступа субъекта персональных данных к его персональным данным, обрабатываемым медучреждением, определяется в соответствии с законодательством и внутренними документами медучреждения.

4.2. Обработка персональных данных.

4.2.1. Обработка персональных данных осуществляется:

– с письменного согласия субъекта персональных данных на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов медучреждения.

Допущенные к обработке персональных данных Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных Работников.

4.2.2. Цели обработки персональных данных:

– обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006 и иными нормативными правовыми актами Российской Федерации;

– осуществление трудовых отношений;

– осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных.

В медучреждении обрабатываются персональные данные следующих субъектов:

– физические лица, состоящие с учреждением в трудовых отношениях;

– физические лица, являющие близкими родственниками сотрудников учреждения;

– физические лица, уволившиеся из учреждения;

– физические лица, являющиеся кандидатами на работу;

– физические лица, состоящие с учреждением в гражданско-правовых отношениях;

– физические лица, обратившиеся в учреждение за медицинской помощью, в том числе законные представители пациентов.

4.2.4. Персональные данные, обрабатываемые медучреждением:

– данные, полученные при осуществлении трудовых отношений;

– данные, полученные для осуществления отбора кандидатов на работу в медучреждение;

– данные, полученные при осуществлении гражданско-правовых отношений;

– данные, полученные при оказании медицинской помощи.

4.2.5. Обработка персональных данных ведется:

– с использованием средств автоматизации;

– без использования средств автоматизации.

4.3. Хранение персональных данных.

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

4.3.2. Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

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

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

4.3.5. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, 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.

4.4. Уничтожение персональных данных.

4.4.1. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

4.4.2. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения персональных данных подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

4.5. Передача персональных данных.

4.5.1. Медучреждение передает персональные данные третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются персональные данные:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального 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, правоохранительные и иные органы в случаях, установленных законодательством.

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов медучреждением создана система защиты персональных данных (далее - СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в

открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

5.5. Основными мерами защиты персональных данных, используемыми медучреждением, являются:

5.5.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите персональных данных;

5.5.2. Определение актуальных угроз безопасности персональных данных при их обработке в ИСПД, и разработка мер и мероприятий по защите персональных данных;

5.5.3. Разработка политики в отношении обработки персональных данных;

5.5.4. Установление правил доступа к персональным данным, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в ИСПД;

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей персональных данных, обеспечение их сохранности;

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

5.5.10. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности персональных данных;

5.5.11. Установление правил доступа к обрабатываемым персональным данным, обеспечение регистрации и учета действий, совершаемых с персональными данными, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

5.5.12. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.5.13. Обучение работников медучреждения, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику медучреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

5.5.14. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта персональных данных и обязанности медучреждения

6.1. Основные права субъекта персональных данных.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место 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;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» или другими федеральными законами.

Субъект персональных данных вправе требовать от медучреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности медучреждения.

Медучреждение обязано:

- при сборе персональных данных предоставить информацию об обработке персональных данных его субъекту по его просьбе;
- в случаях если персональные данные были получены не от субъекта персональных данных уведомить субъекта;
- при отказе в предоставлении персональных данных, субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.