

УТВЕРЖДЕНА
приказом главного врача
ГБУЗ «Балтасинская ЦРБ»
от «10» августа 2026 г. № 268

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Государственного автономного учреждения здравоохранения
«Балтасинская центральная районная больница»

пгт. Балтаси
2026

СОДЕРЖАНИЕ

1. Общие положения
2. Сведения об Операторе
3. Правовые основания обработки персональных данных
4. Основные понятия
5. Категории субъектов, цели обработки и состав персональных данных
6. Принципы и условия обработки персональных данных
7. Согласия субъектов и обработка специальных категорий данных
8. Обработка персональных данных работников и соискателей
9. Передача данных, поручение обработки и раскрытие сведений
10. Локализация и трансграничная передача персональных данных
11. Хранение, уточнение, блокирование, обезличивание и уничтожение
12. Права субъектов и порядок рассмотрения обращений
13. Обязанности Оператора и работников
14. Меры по обеспечению безопасности персональных данных
15. Реагирование на инциденты и утечки персональных данных
16. Контроль, ответственность и обучение
17. Заключительные положения

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в отношении обработки и обеспечения безопасности персональных данных (далее - Политика) определяет цели, принципы, условия и порядок обработки персональных данных в Государственном автономном учреждении здравоохранения «Балтасинская центральная районная больница» (далее - Учреждение, Оператор), а также основные меры по защите прав субъектов персональных данных.

1.2. Политика распространяется на обработку персональных данных с использованием средств автоматизации и без использования таких средств, включая обработку на бумажных носителях, в медицинских, кадровых, бухгалтерских и иных информационных системах, на официальном сайте и официальных страницах Учреждения, а также при использовании систем видеонаблюдения, контроля доступа и записи обращений - если такие системы фактически применяются Оператором.

1.3. Политика применяется в отношении пациентов, их законных представителей и иных лиц, обращающихся за медицинской помощью; работников и бывших работников; соискателей; лиц, работающих по гражданско-правовым договорам; представителей контрагентов; заявителей; посетителей; пользователей официального сайта и иных субъектов, персональные данные которых обрабатывает Оператор.

1.4. Целями Политики являются обеспечение законности обработки персональных данных; защита частной жизни, личной и семейной тайны; сохранение врачебной тайны; предупреждение неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения персональных данных; установление обязанностей и ответственности работников Оператора.

1.5. Персональные данные и сведения, составляющие врачебную тайну, относятся к информации ограниченного доступа. Доступ предоставляется только в пределах должностных обязанностей, законных полномочий и утвержденных прав доступа.

1.6. Политика является общедоступным документом и размещается на официальном сайте Оператора. Если сбор персональных данных осуществляется через информационно-телекоммуникационные сети, доступ к Политике обеспечивается на страницах и в электронных формах, посредством которых осуществляется сбор данных. Дополнительно Политика может размещаться на информационных стендах в местах оказания услуг.

1.7. Конкретные процедуры обработки и защиты персональных данных регулируются приказами, положениями, инструкциями, регламентами, моделями

угроз, перечнями информационных систем и должностей, формами согласий, журналами учета, договорами поручения обработки и иными локальными актами Оператора.

1.8. Настоящая Политика регулирует обработку и защиту персональных данных и не заменяет общую политику информационной безопасности Учреждения. Детальные сведения об архитектуре информационных систем, конфигурации средств защиты и иных мерах, разглашение которых может создать угрозу безопасности, оформляются отдельными внутренними документами ограниченного доступа.

2. СВЕДЕНИЯ ОБ ОПЕРАТОРЕ

2.1. Полное наименование: Государственное автономное учреждение здравоохранения «Балтасинская центральная районная больница».

2.2. Сокращенное наименование: ГАУЗ «Балтасинская ЦРБ».

2.3. Юридический и фактический адрес: 422250, Республика Татарстан, пгт. Балтаси, ул. Ленина, д. 1.

2.4. ИНН 1612000753; КПП 161201001; ОГРН 1021607758446.

2.5. Руководитель Оператора: главный врач Сафаров Рамиль Рафхатович.

2.6. Электронная почта для обращений: baltasi.crb@tatar.ru. Телефон приемной: +7 (84368) 2-62-40. Официальный сайт: <https://zdrav.tatar.ru/crbbaltasi>.

2.7. Лицо, ответственное за организацию обработки персональных данных, назначается приказом главного врача. Полномочия, ответственность и порядок взаимодействия ответственного лица с подразделениями определяются локальными актами Оператора.

2.8. Оператор направляет в Роскомнадзор уведомления, предусмотренные законодательством, и обеспечивает соответствие сведений в реестре операторов фактическим процессам обработки, настоящей Политике и локальным документам.

3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных осуществляется в соответствии с международными договорами Российской Федерации, Конституцией Российской Федерации, федеральными законами и иными нормативными правовыми актами, в том числе:

- Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в действующей редакции;

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральным законом от 03.11.2006 № 174-ФЗ «Об автономных учреждениях»;
- Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федеральным законом от 29.12.2022 № 572-ФЗ - в части использования биометрических персональных данных и идентификации, если соответствующие технологии применяются;
- постановлением Правительства Российской Федерации от 21.03.2012 № 211;
- постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- постановлением Правительства Российской Федерации от 06.07.2008 № 512;
- приказом ФСТЭК России от 18.02.2013 № 21 и Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021;
- приказом ФСБ России от 10.07.2014 № 378 - при использовании средств криптографической защиты информации;
- приказом Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;
- приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»»;
- приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
- приказом Роскомнадзора от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении, о прекращении обработки персональных данных»;
- приказом Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Роскомнадзора с операторами в рамках ведения реестра учета инцидентов в области персональных данных»;

- приказом Роскомнадзора от 19.06.2025 № 140 «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных»;
- нормативными актами Министерства здравоохранения Российской Федерации, регулирующими ведение, предоставление и хранение медицинской документации, включая электронные медицинские документы;
- уставом Оператора, лицензией на осуществление медицинской деятельности, договорами и локальными нормативными актами Оператора.

3.2. При изменении законодательства положения Политики применяются в части, не противоречащей действующим нормам. До внесения изменений Оператор руководствуется актами большей юридической силы.

4. ОСНОВНЫЕ ПОНЯТИЯ

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

Оператор - лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки, состав данных и действия с ними.

Обработка персональных данных - любое действие или совокупность действий с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление и уничтожение.

Автоматизированная обработка - обработка персональных данных с помощью средств вычислительной техники.

Предоставление персональных данных - раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - раскрытие персональных данных неопределенному кругу лиц.

Персональные данные, разрешенные субъектом для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом путем отдельного согласия в порядке статьи 10.1 Федерального закона № 152-ФЗ.

Блокирование - временное прекращение обработки персональных данных, кроме случаев, когда обработка необходима для их уточнения.

Обезличивание - действия, после которых без использования дополнительной информации невозможно определить принадлежность персональных данных конкретному субъекту.

Уничтожение - действия, после которых невозможно восстановить содержание персональных данных в информационной системе и (или) уничтожаются материальные носители.

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

Биометрические персональные данные - сведения о физиологических и биологических особенностях человека, которые используются Оператором для установления личности субъекта.

Специальные категории персональных данных - сведения о расовой или национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья и интимной жизни.

Врачебная тайна - сведения о факте обращения за медицинской помощью, состоянии здоровья, диагнозе и иные сведения, полученные при медицинском обследовании и лечении.

Инцидент - событие, которое привело или может привести к нарушению конфиденциальности, целостности либо доступности персональных данных, включая неправомерную или случайную передачу данных, повлекшую нарушение прав субъектов.

Лицо, осуществляющее обработку по поручению Оператора - лицо, которое обрабатывает персональные данные от имени Оператора на основании договора, государственного контракта или иного предусмотренного законом акта и не определяет собственные цели такой обработки.

5. КАТЕГОРИИ СУБЪЕКТОВ, ЦЕЛИ ОБРАБОТКИ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Пациенты и их представители

5.1.1. Цели обработки: организация записи и приема; оказание медицинской помощи; диагностика, лечение, профилактика, диспансерное наблюдение и медицинская реабилитация; ведение медицинской документации; оформление информированного добровольного согласия или отказа; взаимодействие в системе обязательного и добровольного медицинского страхования; выдача справок, заключений, рецептов и листков нетрудоспособности; проведение экспертиз; рассмотрение обращений; выполнение обязанностей в сфере санитарно-эпидемиологического благополучия, статистического и персонифицированного учета; защита жизни и здоровья; исполнение договоров на платные медицинские услуги.

5.1.2. Могут обрабатываться: фамилия, имя, отчество; пол; дата и место рождения; адрес регистрации и проживания; контактные данные; сведения

документа, удостоверяющего личность; СНИЛС; номер полиса ОМС или ДМС; сведения о законном представителе; сведения о состоянии здоровья, анамнезе, диагнозах, обследованиях, лечении, назначениях, противопоказаниях и нетрудоспособности; изображения и аудиовизуальные материалы - если их получение предусмотрено медицинской технологией или отдельной законной целью; иные данные, необходимые для оказания медицинской помощи и исполнения требований законодательства.

5.1.3. Объем данных определяется конкретной целью и не должен быть избыточным. Использование фотографий, видеозаписей, сведений о диагнозе или иных материалов в информационных, рекламных, образовательных и публичных целях допускается только при наличии отдельного правового основания и требуемого согласия.

5.2. Работники, бывшие работники и лица по гражданско-правовым договорам

5.2.1. Цели обработки: заключение, изменение и прекращение трудовых и гражданско-правовых договоров; кадровый и воинский учет; начисление заработной платы и иных выплат; налоговый и бухгалтерский учет; обязательное социальное и пенсионное страхование; обучение, аттестация и повышение квалификации; охрана труда и обеспечение безопасности; предоставление гарантий и компенсаций; оформление командировок, пропусков, доверенностей и наградений; защита имущества и законных интересов Оператора; архивное хранение документов.

5.2.2. Могут обрабатываться: идентификационные, паспортные, контактные и адресные данные; сведения об образовании, квалификации, трудовой деятельности, воинском учете, семейном положении и иждивенцах - в предусмотренном законом объеме; банковские реквизиты; ИНН; СНИЛС; сведения о медицинских осмотрах и состоянии здоровья только в части, связанной с возможностью выполнения трудовой функции и соблюдением требований охраны труда; сведения о дисциплинарных взысканиях и поощрениях; изображения для пропуска и кадровых документов; иные данные, предусмотренные законодательством и договором.

5.3. Соискатели

5.3.1. Цели обработки: рассмотрение кандидатуры; проверка соответствия квалификационным требованиям; организация собеседований; принятие решения о заключении трудового договора; формирование кадрового резерва - только при отдельном согласии или ином законном основании.

5.3.2. Обрабатываются сведения, содержащиеся в резюме, анкете, документах об образовании и квалификации, контактные данные и иные сведения, непосредственно связанные с предполагаемой трудовой функцией.

5.4. Контрагенты, заявители, посетители и пользователи официальных интернет-ресурсов

5.4.1. Цели обработки: заключение и исполнение договоров; закупочная деятельность; ведение деловой переписки; рассмотрение обращений и запросов; обеспечение пропускного и внутриобъектового режима; защита имущества, жизни и здоровья; обеспечение функционирования официального сайта, электронных форм и обратной связи.

5.4.2. Обрабатываются идентификационные, контактные, должностные и иные данные, необходимые для соответствующей цели. Технические данные пользователей сайта, включая файлы cookie, сетевые идентификаторы, сведения о браузере и устройстве, обрабатываются только в объеме, необходимом для работы сайта, информационной безопасности и статистики, с учетом настроек пользователя и требований законодательства. Необязательные средства аналитики и маркетинга применяются при наличии надлежащего правового основания и информирования пользователя.

5.5. Видеонаблюдение, контроль доступа и запись обращений

5.5.1. Если Оператор осуществляет видеонаблюдение, контроль доступа или запись телефонных и иных обращений, такая обработка производится для обеспечения безопасности, защиты жизни и здоровья, имущества, контроля качества обслуживания и разрешения спорных ситуаций в пределах, установленных законом и локальными актами.

5.5.2. Субъекты информируются о видеонаблюдении и записи понятным способом до входа в зону наблюдения или до начала записи. Системы не должны использоваться в помещениях и ситуациях, где наблюдение несоразмерно цели либо нарушает права граждан. Доступ к записям ограничивается, а сроки хранения устанавливаются локальным актом с учетом цели и рисков.

6. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка осуществляется на законной и справедливой основе для конкретных, заранее определенных и законных целей.

6.2. Не допускаются обработка, несовместимая с целями сбора, объединение баз данных с несовместимыми целями, а также сбор избыточных данных.

6.3. Оператор обеспечивает точность, достаточность и актуальность персональных данных и принимает меры по уточнению или удалению неполных и неточных данных.

6.4. Срок хранения определяется целью обработки, требованиями законодательства, номенклатурой дел, договором или согласием. После

прекращения правовых оснований данные уничтожаются или обезличиваются, если дальнейшее хранение не требуется по закону.

6.5. Обработка допускается при наличии хотя бы одного законного основания, включая согласие субъекта; необходимость исполнения договора; выполнение обязанностей и полномочий Оператора, установленных законом; защиту жизни, здоровья или иных жизненно важных интересов; осуществление правосудия; достижение общественно значимых целей; реализацию законных интересов при условии, что не нарушаются права субъекта.

6.6. Обработка данных о здоровье пациентов осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными сохранять врачебную тайну, либо иными лицами в случаях и порядке, прямо предусмотренных законом.

6.7. Оператор не принимает решения, порождающие юридические последствия для субъекта или иным образом затрагивающие его права и законные интересы, исключительно на основании автоматизированной обработки, кроме случаев, разрешенных законом или основанных на отдельном письменном согласии с предоставлением предусмотренных законом гарантий.

6.8. Работники получают доступ только к тем персональным данным и операциям, которые необходимы для выполнения их должностных обязанностей. Использование данных в личных целях запрещается.

6.9. Сведения, составляющие врачебную тайну, не могут использоваться для продвижения услуг, публикаций, обучения, научных исследований или статистики вне предусмотренных законом оснований. При возможности применяются обезличивание и минимизация данных.

7. СОГЛАСИЯ СУБЪЕКТОВ И ОБРАБОТКА СПЕЦИАЛЬНЫХ КАТЕГОРИЙ ДАННЫХ

7.1. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие оформляется отдельно от иных информации и документов, которые субъект подтверждает или подписывает.

7.2. В случаях, когда законом требуется письменная форма, согласие содержит сведения, предусмотренные статьей 9 Федерального закона № 152-ФЗ, и подписывается субъектом или его представителем собственноручно либо электронной подписью в установленном порядке. Оператор обязан хранить доказательства получения согласия.

7.3. Не допускается подмена одного вида волеизъявления другим. Отдельно оформляются, когда они необходимы:

- согласие на обработку персональных данных;
- информированное добровольное согласие на медицинское вмешательство или отказ от него;
- согласие на обработку персональных данных, разрешенных для распространения;
- согласие на фото-, видео- или аудиосъемку и использование материалов вне оказания медицинской помощи;
- согласие на получение рекламных, информационных и иных необязательных рассылок.

7.4. Согласие на распространение персональных данных оформляется отдельно от иных согласий в соответствии со статьей 10.1 Федерального закона № 152-ФЗ и требованиями Роскомнадзора. Субъект вправе установить запреты и условия обработки неограниченным кругом лиц. Молчание или бездействие не признаются согласием.

7.5. Согласие может быть отозвано. Отзыв не прекращает обработку, если у Оператора сохраняется иное законное основание, включая обязанности по хранению медицинской, кадровой, бухгалтерской или архивной документации.

7.6. Персональные данные преимущественно получают у самого субъекта или его законного представителя. При получении данных от третьего лица субъект уведомляется в случаях и порядке, установленных законом.

7.7. Специальные категории персональных данных обрабатываются только при наличии оснований, прямо установленных законом. Сведения о здоровье пациентов обрабатываются в объеме, необходимом для организации и оказания медицинской помощи и исполнения обязанностей медицинской организации.

7.8. Фотография, видеозапись, голос или иные физиологические характеристики признаются биометрическими персональными данными только тогда, когда Оператор использует их для установления личности. Такая обработка осуществляется при наличии письменного согласия либо иного предусмотренного законом основания.

7.9. Обработка персональных данных несовершеннолетних, недееспособных и ограниченно дееспособных лиц осуществляется с участием законных представителей в случаях, предусмотренных законодательством, с учетом права пациента на медицинскую тайну и самостоятельное принятие решений в установленном законом возрасте и объеме.

8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И СОИСКАТЕЛЕЙ

8.1. Оператор получает от работника только данные, необходимые для трудовых отношений, обеспечения безопасных условий труда, предоставления гарантий, расчета выплат и исполнения обязанностей работодателя.

8.2. Согласие работника не требуется, когда обработка прямо предусмотрена трудовым, налоговым, пенсионным, социальным и иным законодательством либо необходима для исполнения трудового договора. Если законного основания без согласия нет, согласие оформляется отдельным документом.

8.3. Работник знакомится под подпись с локальными актами, регуливающими обработку его персональных данных, и обязан сообщать об изменении сведений, влияющих на исполнение трудового договора и предоставление гарантий.

8.4. Передача данных работника третьим лицам без его согласия допускается только в случаях, прямо предусмотренных законом, включая передачу налоговым органам, Социальному фонду России, военным комиссариатам, органам государственного контроля, правоохранительным и судебным органам, а также банкам для выплаты заработной платы при наличии надлежащего правового основания.

8.5. При привлечении внешних организаций для кадрового, бухгалтерского, юридического, архивного, информационно-технологического или иного обслуживания заключается договор поручения обработки персональных данных, отвечающий требованиям закона и раздела 9 настоящей Политики.

8.6. Данные соискателя хранятся в течение срока, необходимого для принятия решения. При отказе в приеме и отсутствии согласия на кадровый резерв данные уничтожаются не позднее 30 календарных дней после принятия решения, если закон не требует их дальнейшего хранения.

8.7. Включение соискателя в кадровый резерв допускается только на основании отдельного согласия или иного законного основания с указанием срока хранения и порядка исключения из резерва.

8.8. Запрос сведений о соискателе у прежних работодателей и иных лиц допускается при наличии согласия соискателя или иного законного основания.

9. ПЕРЕДАЧА ДАННЫХ, ПОРУЧЕНИЕ ОБРАБОТКИ И РАСКРЫТИЕ СВЕДЕНИЙ

9.1. Предоставление персональных данных третьим лицам производится с согласия субъекта либо без согласия в случаях, прямо предусмотренных законом, в объеме, соответствующем цели запроса.

9.2. Сведения, составляющие врачебную тайну, предоставляются без согласия пациента только по основаниям и в порядке, установленным Федеральным законом № 323-ФЗ и иными федеральными законами. Каждый запрос оценивается на предмет полномочий заявителя, цели, правового основания и объема запрашиваемых сведений.

9.3. Передача данных по запросу оформляется и учитывается способом, позволяющим установить дату, получателя, правовое основание, состав переданных данных и ответственное лицо. Необоснованные запросы подлежат мотивированному отклонению.

9.4. При поручении обработки другому лицу договор, государственный контракт или иной акт должен определять:

- перечень персональных данных и категории субъектов;
- перечень действий с данными, цели и способы обработки;
- обязанность соблюдать конфиденциальность и требования к безопасности;
- требование о локализации баз данных и месте обработки, когда оно применимо;
- условия привлечения субподрядчиков и запрет их привлечения без согласованного порядка;
- порядок взаимодействия при запросах субъектов и требованиях Роскомнадзора;
- обязанность незамедлительно уведомлять Оператора об инцидентах, ошибочной передаче, утрате доступа и иных нарушениях;
- порядок возврата, блокирования и уничтожения данных после прекращения договора, включая подтверждение уничтожения;
- обязанность предоставлять подтверждение принятых мер защиты и право Оператора проводить контроль исполнения условий поручения.

9.5. Лицо, обрабатывающее данные по поручению, не определяет цели обработки и не использует данные в собственных интересах. Оператор контролирует соблюдение условий поручения в пределах, установленных договором и законом.

9.6. Передача данных через незащищенные каналы связи, личные адреса электронной почты, общедоступные мессенджеры, личные облачные хранилища и несанкционированные съемные носители запрещается, если иной защищенный порядок не установлен локальными актами и не обеспечены требования законодательства.

9.7. Публикация сведений о работниках, пациентах и иных субъектах на сайте, стендах, в социальных сетях, СМИ и иных открытых источниках допускается только при наличии законного основания и, когда требуется, отдельного согласия на распространение персональных данных.

9.8. Передача персональных данных органам власти и организациям посредством государственных информационных систем, межведомственного взаимодействия и защищенных каналов осуществляется в соответствии с установленными регламентами и полномочиями.

10. ЛОКАЛИЗАЦИЯ И ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. При сборе персональных данных граждан Российской Федерации, в том числе через сеть Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение и извлечение таких данных с использованием баз данных, находящихся на территории Российской Федерации, кроме установленных законом исключений.

10.2. Использование иностранных облачных сервисов, программ, коммуникационных платформ и иных ресурсов для обработки персональных данных допускается только после документированной правовой и технической оценки, проверки соблюдения требования локализации и принятия решения уполномоченным лицом Оператора.

10.3. По общему правилу Оператор не осуществляет трансграничную передачу персональных данных. До начала такой передачи Оператор направляет отдельное уведомление в Роскомнадзор, получает от иностранного получателя необходимые сведения, оценивает правовые основания, риски и меры защиты и оформляет решение в установленном порядке.

10.4. Трансграничная передача прекращается при запрете или ограничении Роскомнадзора, утрате правового основания, нарушении получателем условий обработки либо возникновении неприемлемого риска для прав субъектов.

11. ХРАНЕНИЕ, УТОЧНЕНИЕ, БЛОКИРОВАНИЕ, ОБЕЗЛИЧИВАНИЕ И УНИЧТОЖЕНИЕ

11.1. Бумажные документы хранятся в помещениях, шкафах, сейфах и иных местах хранения, исключающих доступ посторонних лиц, утрату, повреждение и несанкционированное копирование. Электронные данные хранятся в утвержденных информационных системах с разграничением доступа, регистрацией действий и резервным копированием.

11.2. Сроки хранения определяются законодательством, перечнями архивных документов, правилами ведения медицинской документации, номенклатурой дел, договорами и целями обработки. Срок действия согласия не сокращает обязательные сроки хранения, установленные законом.

11.3. При выявлении неточных данных Оператор блокирует их на период проверки, если это не нарушает права субъекта или третьих лиц, и в течение семи

рабочих дней после получения подтверждающих сведений уточняет данные либо обеспечивает их уточнение.

11.4. При выявлении неправомерной обработки Оператор прекращает ее или обеспечивает прекращение в срок, установленный законом. Если обеспечить правомерность невозможно, данные уничтожаются в установленный законом срок.

11.5. По достижении цели обработки или при отзыве согласия данные уничтожаются в срок, установленный законом, если отсутствуют иные основания для обработки. При технической невозможности немедленного уничтожения данные блокируются и уничтожаются не позднее предельного срока, установленного законом.

11.6. Уничтожение оформляется актом и (или) выгрузкой из журнала регистрации событий информационной системы в соответствии с требованиями Роскомнадзора. Способ уничтожения должен исключать восстановление данных.

11.7. Обезличивание применяется для статистических, научных, аналитических и иных законных целей. Методы обезличивания выбираются с учетом риска повторной идентификации и требований Роскомнадзора. Дополнительная информация, позволяющая восстановить связь с субъектом, хранится отдельно и защищается.

11.8. Вынос оригиналов документов и носителей за пределы помещений Оператора допускается только по служебной необходимости, с разрешения уполномоченного лица и с регистрацией передачи.

11.9. Резервные копии персональных данных учитываются при определении сроков хранения и уничтожения. Процедуры резервного копирования должны обеспечивать возможность восстановления данных и контролируемое удаление копий после прекращения правовых оснований.

12. ПРАВА СУБЪЕКТОВ И ПОРЯДОК РАССМОТРЕНИЯ ОБРАЩЕНИЙ

12.1. Субъект вправе получить сведения об обработке его персональных данных, включая подтверждение факта обработки, правовые основания и цели, способы обработки, состав данных и источник их получения, сроки обработки и хранения, сведения о получателях и лицах, действующих по поручению, информацию о трансграничной передаче и порядке реализации своих прав.

12.2. Субъект вправе требовать уточнения, блокирования или уничтожения данных, если они неполные, устаревшие, неточные, незаконно полученные или не нужны для заявленной цели; отозвать согласие; установить запреты на распространение; обжаловать действия Оператора в Роскомнадзор или суд; требовать возмещения убытков и компенсации морального вреда в предусмотренных законом случаях.

12.3. Запрос должен позволять идентифицировать заявителя и подтверждать его отношение к данным. Представитель дополнительно предъявляет документ, подтверждающий полномочия. Запрос может быть подан на бумаге или в форме электронного документа, подписанного электронной подписью, если такая подпись требуется законом.

12.4. Оператор предоставляет ответ в доступной форме в срок не более десяти рабочих дней с даты обращения или получения запроса. Срок может быть продлен не более чем на пять рабочих дней при направлении мотивированного уведомления с указанием причин продления.

12.5. Отказ в предоставлении сведений должен быть мотивирован и содержать ссылку на закон. В ответ не включаются персональные данные других лиц, если отсутствует законное основание для их раскрытия.

12.6. Пациент или его законный представитель получает медицинские документы, их копии и выписки в порядке и сроки, установленные законодательством об охране здоровья и локальными регламентами Оператора.

12.7. Обращения регистрируются, передаются ответственному лицу и рассматриваются с участием подразделений, фактически осуществляющих обработку. Результаты рассмотрения и принятые меры документируются.

13. ОБЯЗАННОСТИ ОПЕРАТОРА И РАБОТНИКОВ

13.1. Оператор обязан:

- назначить лицо, ответственное за организацию обработки персональных данных, и определить его полномочия;
- издать локальные акты по вопросам обработки и защиты персональных данных и обеспечивать их актуальность;
- определить перечни обрабатываемых данных, категории субъектов, цели, способы, сроки хранения, информационные системы и лиц, имеющих доступ;
- проводить оценку вреда, который может быть причинен субъектам при нарушении закона, и соотносить вред с принимаемыми мерами;
- обеспечивать соответствие уведомления Роскомнадзора фактическим процессам и направлять уведомления о начале, изменении, прекращении обработки, трансграничной передаче и инцидентах в предусмотренных случаях;
- получать согласия в надлежащей форме, отдельно от иных документов, и хранить доказательства их получения;
- осуществлять внутренний контроль и аудит соответствия обработки требованиям законодательства и локальных актов;
- обеспечивать обучение и ознакомление работников, допущенных к обработке персональных данных;

- рассматривать запросы субъектов и требования Роскомнадзора в установленные сроки;
- обеспечивать безопасность данных и документально подтверждать принятые меры;
- проверять договоры с обработчиками, поставщиками информационных систем, хостинга, технической поддержки, архивного и иного обслуживания.

13.2. Работник, имеющий доступ к персональным данным, обязан:

- использовать данные только для выполнения служебных обязанностей и в пределах предоставленных прав;
- соблюдать врачебную, служебную и иную охраняемую законом тайну;
- не передавать логины, пароли, ключи электронной подписи и носители другим лицам;
- не копировать, не фотографировать и не выносить данные без разрешения;
- немедленно сообщать ответственному лицу о потере документов или носителей, ошибочной отправке, фишинге, вредоносном программном обеспечении, подозрении на несанкционированный доступ и иных инцидентах;
- соблюдать правила работы с бумажными документами, электронной почтой, съемными носителями, медицинскими информационными системами и удаленным доступом;
- блокировать рабочий сеанс при оставлении рабочего места и не оставлять документы доступными посторонним;
- после прекращения полномочий не раскрывать сведения, ставшие известными в связи с работой.

14. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Оператор принимает правовые, организационные и технические меры, соответствующие характеру данных, способам обработки, актуальным угрозам, возможному вреду субъектам и установленному уровню защищенности информационных систем.

14.2. Организационные меры включают:

- назначение ответственных лиц и распределение полномочий;
- инвентаризацию процессов обработки, информационных систем, баз данных, носителей и каналов передачи;
- утверждение перечня должностей и матрицы доступа по принципу минимальных привилегий;
- регламентацию допуска в помещения, выдачи ключей и доступа к архивам;

- учет носителей, документов, запросов, выдачи сведений, уничтожения и инцидентов;
- проверку контрагентов и условий договоров поручения обработки;
- обучение работников, проверку знаний и проведение практических тренировок по реагированию на инциденты;
- периодический внутренний контроль и пересмотр модели угроз и мер защиты.

14.3. Технические меры включают в применимом объеме:

- идентификацию и аутентификацию пользователей, индивидуальные учетные записи и многофакторную аутентификацию для критичных систем, если это технически возможно;
- разграничение прав доступа, блокировку неиспользуемых учетных записей и своевременное прекращение доступа уволенных или переведенных работников;
- регистрацию и анализ событий безопасности, синхронизацию времени и хранение журналов;
- защиту от вредоносного кода, межсетевое экранирование, сегментацию сети, фильтрацию электронной почты и веб-трафика;
- установку обновлений безопасности и управление уязвимостями;
- резервное копирование, регулярную проверку восстановления и защищенное хранение резервных копий;
- криптографическую защиту при передаче по открытым каналам и на мобильных носителях, когда она требуется;
- защиту рабочих станций, серверов, медицинского оборудования и удаленного доступа;
- контроль съемных носителей и периферийных устройств;
- физическую защиту помещений, серверных, архивов и мест хранения документов;
- безопасное удаление данных и утилизацию носителей.

14.4. Пароли должны быть уникальными, не передаваться другим лицам и изменяться при компрометации. Использование одной учетной записи несколькими работниками не допускается, кроме технологических учетных записей, для которых установлен отдельный контролируемый порядок.

14.5. Удаленный доступ к информационным системам с персональными данными разрешается только через утвержденные защищенные средства, с регистрацией действий и при наличии служебной необходимости.

14.6. Использование личных устройств для обработки персональных данных допускается только при наличии утвержденного порядка, технической защиты и разрешения Оператора. Самовольное хранение рабочих данных на личных устройствах запрещается.

14.7. Рабочие места, на которых обрабатываются персональные данные, должны быть защищены от визуального доступа посторонних лиц. При уходе работник блокирует сеанс, а бумажные документы убирает в закрываемое место хранения.

14.8. Меры защиты пересматриваются при изменении информационных систем, технологий, состава данных, выявлении новых угроз, инциденте или изменении законодательства.

15. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ И УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. Каждый работник обязан незамедлительно сообщить о возможном инциденте своему руководителю, ответственному за организацию обработки персональных данных и подразделению, отвечающему за информационную безопасность. Самостоятельное сокрытие, удаление следов или публичное комментирование инцидента запрещается.

15.2. Оператор организует локализацию инцидента, сохранение доказательств, анализ причин и последствий, определение состава затронутых данных и субъектов, восстановление работоспособности и принятие мер по недопущению повторения.

15.3. При установлении факта неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов, Оператор направляет в Роскомнадзор первичное уведомление в течение 24 часов и дополнительное уведомление о результатах внутреннего расследования в течение 72 часов с момента выявления инцидента.

15.4. Лица, обрабатывающие данные по поручению Оператора, обязаны уведомлять Оператора об инциденте незамедлительно и предоставлять сведения, необходимые для исполнения Оператором обязанностей в установленные законом сроки.

15.5. Взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак и иными уполномоченными органами осуществляется только в случаях, когда соответствующая обязанность установлена законодательством, в том числе законодательством о безопасности критической информационной инфраструктуры, либо по требованию уполномоченного органа.

15.6. Решение об уведомлении затронутых субъектов принимается с учетом требований закона, характера данных, вероятности и тяжести вреда и рекомендаций уполномоченных органов. Уведомление не должно раскрывать дополнительные персональные данные или технические сведения, создающие новые риски.

15.7. По итогам инцидента оформляются материалы расследования, корректирующие мероприятия, изменения в модели угроз, регламенты и программы обучения. Выполнение мероприятий контролируется ответственным лицом.

16. КОНТРОЛЬ, ОТВЕТСТВЕННОСТЬ И ОБУЧЕНИЕ

16.1. Внутренний контроль проводится планово и внепланово. Основаниями для внеплановой проверки являются инцидент, жалоба субъекта, требование надзорного органа, существенное изменение информационной системы или выявление нарушения.

16.2. Контроль включает проверку законности целей и состава данных, форм согласий, сроков хранения, разграничения доступа, журналов событий, договоров с обработчиками, готовности к реагированию на инциденты, фактического уничтожения и актуальности уведомлений Роскомнадзора.

16.3. Работники проходят вводное обучение до предоставления доступа к персональным данным и периодическое обучение не реже одного раза в год, а также внеплановое обучение после существенных изменений законодательства, процессов обработки или инцидентов.

16.4. Лица, виновные в нарушении требований к обработке и защите персональных данных, несут дисциплинарную, материальную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством.

16.5. Нарушение Политики может являться основанием для ограничения или прекращения доступа к информационным системам, проведения служебной проверки и применения мер ответственности.

17. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

17.1. Политика вступает в силу со дня утверждения приказом главного врача и действует до ее отмены или утверждения новой редакции.

17.2. Со дня вступления в силу настоящей Политики Политика безопасности персональных данных, утвержденная 26 июля 2017 года, признается утратившей силу.

17.3. Проверка актуальности Политики проводится не реже одного раза в год. Политика пересматривается при изменении законодательства, структуры и деятельности Оператора, состава информационных систем и обрабатываемых данных, по результатам проверок, оценки рисков или расследования инцидента. При отсутствии оснований для изменения результат ежегодной проверки документируется.

17.4. Ответственное лицо организует размещение актуальной редакции на официальном сайте и информационных стендах, а также ознакомление работников, имеющих доступ к персональным данным.

17.5. Формы согласий, уведомлений, запросов, актов уничтожения, журналы учета, инструкции и другие приложения утверждаются отдельными локальными актами и должны соответствовать действующему законодательству и настоящей Политике.

17.6. Вопросы, не урегулированные Политикой, разрешаются в соответствии с законодательством Российской Федерации и локальными нормативными актами Оператора.

17.7. Контактный адрес для обращений субъектов: 422250, Республика Татарстан, пгт. Балтаси, ул. Ленина, д. 1. Электронная почта: baltasi.crb@tatar.ru. Телефон приемной: +7 (84368) 2-62-40.

