

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГАУЗ «ГОРОДСКАЯ ДЕТСКАЯ БОЛЬНИЦА № 1» Г. КАЗАНИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в отношении обработки и защиты персональных данных (далее - Политика) разработана в соответствии с Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основным внутренним нормативным актом, определяющим порядок обработки, хранения, передачи и защиты персональных данных в Государственном автономном учреждении здравоохранения «Городская детская больница № 1» г. Казани (далее - ГДБ № 1, Оператор).

1.2. Настоящая Политика разработана в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, врачебную тайну, а также установления ответственности должностных лиц ГДБ № 1 за несоблюдение требований законодательства РФ.

1.3. Действие настоящей Политики распространяется на все процессы обработки персональных данных, осуществляемые ГДБ № 1 как с использованием средств вычислительной техники (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка).

1.4. Реквизиты и сведения об Операторе персональных данных:

- Полное наименование: Государственное автономное учреждение здравоохранения «Городская детская больница № 1» г. Казани
- Сокращенное наименование: ГАУЗ «ГДБ № 1» г. Казани
- ИНН: 1658022679 / КПП: 165801001
- Юридический и фактический адрес: 420034, Республика Татарстан, г. Казань, ул. Декабристов, д. 125А
- Регистрационный номер в реестре операторов Роскомнадзора: 16-0024310

1.5. Правовыми основаниями обработки персональных данных в ГДБ № 1 являются:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Семейный кодекс Российской Федерации;
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 18.11.2020 № 1853 «Об утверждении Правил предоставления гостиничных услуг в Российской Федерации»;
- Приказ Минтруда России от 19.05.2021 № 320н «Об утверждении формы, порядка ведения и хранения трудовых книжек»;
- Приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;
- Приказ Роскомнадзора от 28.10.2022 № 178 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
- Устав ГДБ № 1, лицензии на осуществление медицинской деятельности, а также согласия субъектов на обработку персональных данных.

2. ТЕРМИНЫ И ПРИНЯТЫЕ СОКРАЩЕНИЯ

- Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- Специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости.
- Врачебная тайна — факт обращения гражданина за оказанием медицинской помощи, состояние его здоровья и диагноз, иные сведения, полученные при его медицинском обследовании и лечении.
- 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.
- Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.
- 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 невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.
- Информационная система персональных данных (ИСПДн) — 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.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. ГДБ № 1 осуществляет обработку персональных данных исключительно для достижения конкретных, заранее определенных и законных целей:

- Оказание первичной медико-санитарной, специализированной, в том числе высокотехнологичной, медицинской помощи населению;
- Установление медицинского диагноза, оказание медицинских и медико-социальных услуг;
- Ведение учета медицинской документации, составление статистической отчетности в сфере здравоохранения;
- Выполнение функций, обязанностей и полномочий работодателя в соответствии с трудовым, пенсионным, налоговым законодательством РФ и законодательством об обязательном социальном страховании;
- Содействие работникам в трудоустройстве, обучении, продвижении по службе, обеспечение личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- Подбор персонала (рассмотрение кандидатов на замещение вакантных должностей);
- Ведение воинского учета сотрудников;
- Взаимодействие со страховыми медицинскими организациями в системе ОМС и ДМС;
- Осуществление информационного взаимодействия с Единой государственной информационной системой в сфере здравоохранения (ЕГИСЗ) и Государственной информационной системой ОМС;
- Обеспечение обратной связи с гражданами, включая запись на прием к врачу и обработку электронных обращений через официальный сайт ГДБ № 1 в сети «Интернет»;

- Исполнение судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством РФ.

4. КАТЕГОРИИ СУБЪЕКТОВ И СОСТАВ ОБРАБАТЫВАЕМЫХ ДАННЫХ

4.1. В ГДБ № 1 обрабатываются персональные данные следующих категорий субъектов:

4.1.1. Работники ГДБ № 1 (включая бывших работников):

- Фамилия, имя, отчество, дата и место рождения, гражданство;
- Паспортные данные (серия, номер, кем и когда выдан, код подразделения);
- Адрес места жительства (по регистрации и фактический), контактный телефон, адрес электронной почты;
- ИНН, СНИЛС, реквизиты полиса ОМС;
- Сведения об образовании, квалификации, специальности, наличии специальных знаний или специальной подготовки, сертификатах и аккредитации специалиста;
- Сведения о трудовой деятельности, трудовом стаже, предыдущих местах работы;
- Сведения о семейном положении, составе семьи, близких родственниках (в объемах, необходимых для предоставления льгот);
- Сведения о воинском учете;
- Сведения о заработной плате, доходах, банковских реквизитах для перечисления денежных средств;
- Сведения о прохождении обязательных медицинских осмотров и вакцинации.

4.1.2. Соискатели на замещение вакантных должностей:

- Фамилия, имя, отчество, дата рождения, контактные данные;
- Сведения об образовании, квалификации, стаже работы, биографические данные, содержащиеся в резюме.

4.1.3. Пациенты и их законные представители:

- Фамилия, имя, отчество пациента и законного представителя (родителя, опекуна);
- Дата рождения, пол, место жительства и регистрации;
- Паспортные данные законного представителя / Данные свидетельства о рождении или паспорта пациента;
- Реквизиты полиса ОМС/ДМС, СНИЛС;
- Сведения о состоянии здоровья, анамнезе, симптомах, медицинском диагнозе, проведенных обследованиях, назначенных и выполненных медицинских вмешательствах, результаты лабораторных и инструментальных исследований;
- Контактные номера телефонов и адрес электронной почты.

4.1.4. Пользователи официального сайта ГДБ № 1:

- Фамилия, имя, отчество;
- Контактный номер телефона, адрес электронной почты;
- Текст обращения или параметры записи на прием к врачу.

4.2. Особенности обработки данных пользователей официального сайта: Обработка персональных данных пользователей сайта осуществляется исключительно для целей обеспечения обратной связи и записи на прием. На официальном сайте ГДБ № 1 не используются элементы сторонних иностранных метрических систем и систем веб-аналитики (Google Analytics, Matomo и др.). Сбор информации через веб-формы осуществляется только после получения явного согласия пользователя путем проставления независимой отметки (чекбокса).

5. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ И ОПЕРАТОРА

5.1. Субъект персональных данных имеет право:

- Получать информацию, касающуюся обработки его персональных данных, в порядке и в сроки, предусмотренные ст. 14 152-ФЗ;
- Требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- Отозвать согласие на обработку персональных данных;
- Обжаловать действия или бездействие Оператора в Роскомнадзор или в судебном порядке;
- На защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

5.2. Регламент рассмотрения запросов субъектов ПДн: Оператор предоставляет ответ на официальный запрос субъекта ПДн или его представителя в течение 10 (десяти) рабочих дней с момента обращения. Указанный срок может быть продлен не более чем на 5 (пять) рабочих дней при направлении Оператором мотивированного уведомления с указанием причин продления.

5.3. Оператор обязан:

- Организовывать обработку персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ;
- Разъяснять субъекту ПДн юридические последствия отказа предоставить его персональные данные;
- Принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа;
- Назначить ответственного за организацию обработки персональных данных;
- Опубликовать настоящую Политику в открытом доступе на официальном сайте ГДБ № 1 в сети «Интернет».

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных осуществляется с согласия субъекта на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации.

6.2. Обработка специальных категорий персональных данных (данных о состоянии здоровья пациентов) осуществляется без согласия субъекта, если обработка осуществляется в медицинских целях, для установления медицинского

диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну (ч. 2 ст. 10 152-ФЗ, ст. 13 323-ФЗ).

6.3. Передача персональных данных третьим лицам: ГДБ № 1 не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, прямо установленных законодательством РФ, включая передачу сведений в:

- Министерство здравоохранения Республики Татарстан;
- Территориальный фонд обязательного медицинского страхования (ТФОМС) и страховые медицинские организации;
- Фонд пенсионного и социального страхования РФ (СФР);
- Федеральную службу по надзору в сфере здравоохранения (Росздравнадзор);
- Правоохранительные органы, органы прокуратуры, суда и следствия по официальным запросам.

7. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

7.1. Обработка персональных данных на бумажных носителях осуществляется в соответствии с Постановлением Правительства РФ от 15.09.2008 № 687.

7.2. Персональные данные при их неавтоматизированной обработке должны отделяться от иной информации, в частности путем фиксации их на отдельных материальных носителях (медицинские карты, личные дела сотрудников, журналы).

7.3. Личные дела сотрудников, медицинские карты пациентов, журналы учета и архивные документы хранятся в запирающихся шкафах и сейфах в помещениях с ограниченным доступом, исключающим возможность бесконтрольного проникновения третьих лиц.

8. СРОКИ ХРАНЕНИЯ И ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Сроки хранения персональных данных на бумажных и электронных носителях определяются в соответствии с Приказом Росархива от 20.12.2019 № 236, Приказом Минтруда России от 19.05.2021 № 320н и нормативно-правовыми актами Минздрава России:

- Медицинская документация стационара — 25 лет;
- Медицинские карты амбулаторных больных — 25 лет;
- Личные дела и личные карточки сотрудников — 50/75 лет;
- Согласия на обработку ПДн — 3 года после истечения срока действия или отзыва.

8.2. Порядок уничтожения персональных данных: При достижении целей обработки, истечении срока хранения или при отзыве согласия субъектом персональные данные подлежат уничтожению в течение 30 (тридцати) дней, если иное не предусмотрено законодательством.

8.3. Уничтожение персональных данных осуществляется Комиссией по уничтожению персональных данных, назначаемой

приказом главного врача, в соответствии с требованиями Приказа Роскомнадзора от 28.10.2022 № 178:

- Для бумажных носителей: уничтожение методом бумагорезания (шредирования) или сжигания, исключающим возможность восстановления текста, с составлением Акта об уничтожении персональных данных;
- Для электронных носителей: гарантированное стирание файлов из баз данных и ИСПДн с формированием выгрузки из журнала регистраций событий в информационной системе.

9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

9.1. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты информации, нейтрализующей актуальные угрозы в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119.

9.2. Обязательные организационные и технические меры включают:

- Назначение лица, ответственного за организацию обработки и безопасность ПДн;
- Разграничение прав доступа пользователей к ИСПДн;
- Использование сертифицированных средств защиты информации и антивирусного ПО;
- Учет машинных носителей персональных данных;
- Регулярное резервное копирование баз данных.

9.3. Регламент информирования о компьютерных инцидентах (утечках): В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов ПДн, ГДБ № 1 обязано:

- В течение 24 часов уведомить Роскомнадзор о произошедшем инциденте, его причинах, предполагаемом вреде и принятых мерах;
- В течение 72 часов провести внутреннее расследование и представить в Роскомнадзор результаты расследования с указанием лиц, допустивших нарушение.

10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Должностные лица и работники ГДБ № 1, имеющие доступ к персональным данным и виновные в нарушении требований законодательства Российской Федерации в области обработки и защиты персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящая Политика вступает в силу с момента ее утверждения главным врачом ГДБ № 1 и действует бессрочно до замены ее новой редакцией.

11.2. Политика подлежит актуализации в случае изменения законодательства Российской Федерации в области персональных данных или изменения внутренних процессов обработки данных в ГДБ № 1.

11.3. Действующая версия настоящей Политики в обязательном порядке размещается в свободном доступе на официальном сайте ГАУЗ «Городская детская больница № 1» г. Казани в сети «Интернет».