

«УТВЕРЖДАЮ»



**Политика Государственного автономного учреждения
здравоохранения Республики Башкортостан Стоматологическая
Поликлиника № 8 города Уфа**

в области обработки и защиты персональных данных

(в редакции от 11.01.2016г.)

Уфа, 2016г.

1. Назначение

1.1. Настоящий документ определяет политику Государственного автономного учреждения здравоохранения Республики Башкортостан Стоматологическая Поликлиника № 8 города Уфа (далее – Оператор) в отношении обработки персональных данных (далее – ПДн).

1.2. Настоящая политика в области обработки и защиты ПДн (далее – Политика) разработана в соответствии с п. 2 ст. 18.1 Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных, обрабатываемых Оператором.

1.3. Целью настоящей Политики является защита интересов Оператора, его работников, субъектов ПДн, обрабатываемых Оператором, а также исполнение законодательства Российской Федерации о персональных данных.

1.4. Политика распространяется на Данные полученные как до, так и после подписания настоящей Политики.

2. Общие положения

2.1. В целях поддержания деловой репутации и гарантирования выполнения норм федерального законодательства в полном объеме Оператор считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

2.2. Политика характеризуется следующими признаками:

2.2.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки ПДн субъектов персональных данных.

2.2.2. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором ПДн, права и обязанности оператора при обработке ПДн, права субъектов ПДн, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности ПДн при их обработке.

2.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке ПДн.

2.3. Действие настоящего документа распространяется на все процессы, в рамках которых осуществляется обработка персональных данных субъектов ПДн всех категорий.

3. Информация об Операторе

Наименование: Государственное автономное учреждение здравоохранения Республики Башкортостан Стоматологическая Поликлиника № 8 города Уфа.

ИНН: 0278067696

Фактический адрес: 450059, РБ, г.Уфа, ул. Рихарда Зорге, д.20

Тел., факс: (347) 282-98-68

e-mail: ufa.sp8@doctorrb.ru,

Реестр операторов персональных данных: <http://rkn.gov.ru/personal-data/register/?id=08-0010732>, Приказ № 109 от 07.03.2013г.

4. Правовые основания обработки персональных данных

4.1. Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

4.1.1. Конституцией Российской Федерации.

- 4.1.2. Трудовым кодексом Российской Федерации.
- 4.1.3. Гражданским кодексом Российской Федерации.
- 4.1.4. Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- 4.1.5. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
- 4.1.6. Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- 4.1.7. Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- 4.1.8. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- 4.1.9. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 4.1.10. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- 4.1.11. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- 4.2. Во исполнение настоящей Политики Оператором утверждены следующие локальные нормативные правовые акты:
 - 4.2.1. Концепция информационной безопасности информационных систем персональных данных ГАУЗ РБ Стоматологическая Поликлиника № 8 г.Уфа;
 - 4.2.2. Положение по защите персональных данных в Государственном автономном учреждении здравоохранения Стоматологическая Поликлиника № 8 городского округа город Уфа Республики Башкортостан.
 - 4.2.3. Положение по обработке персональных данных работников в Государственном автономном учреждении здравоохранения Стоматологическая Поликлиника № 8 городского округа город Уфа Республики Башкортостан.
 - 4.2.3. Положение по обработке персональных данных пациентов в Государственном автономном учреждении здравоохранения Стоматологическая Поликлиника № 8 городского округа город Уфа Республики Башкортостан.
 - 4.2.4. План мероприятий по внутреннему контролю за соблюдением безопасности персональных данных ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;
 - 4.2.5. Аналитическое обоснование необходимости создания системы защиты информации ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;
 - 4.2.6. Положение о комиссии по классификации информационных систем персональных данных ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;
 - 4.2.7. Положение о разграничении прав доступа к персональным данным ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;
 - 4.2.8. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;
 - 4.2.9. Приказы о назначении ответственных лиц за работу с персональными данными сотрудников, за компьютерную обработку персональных данных пациентов, за обеспечением информационной безопасности.
 - 4.2.10. Порядок доступа работников Оператора к сведениям конфиденциального характера.
 - 4.2.11. Перечень обрабатываемых персональных данных.

4.2.12. Перечень должностей, работников, допущенных к обработке персональных данных.

4.3. Разработны и утверждены:

4.3.1. Иструкции: администратора безопасности информационных систем персональных данных, по обеспечению безопасности рабочих мест обработки персональных данных, о порядке проведения разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, по обработке персональных данных без использования средств автоматизации, по работе с обращениями субъектов персональных данных, о порядке физической охраны помещений, содержащих носители персональных данных, по работе со съемными носителями, содержащими персональные данные, пользователя информационной системы персональных данных ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;

4.3.2. Журналы: учета антивирусных проверок, учета логинов, учета мероприятий по контролю, учета обращений субъектов персональных данных, учета резервного копирования защищаемой информации, учета средств защиты информации, учета съемных носителей, содержащих персональные данные ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;

4.3.3. Частная модель актуальных угроз информационной системы персональных данных «Пациенты», Частная модель актуальных угроз информационной системы персональных данных «Сотрудники», Частная модель нарушителя информационных систем персональных данных ГАУЗ РБ Стоматологическая поликлиника № 8 г.Уфа;

4.3.6. Регламенты взаимодействия с субъектами персональных данных (запросы);

4.2.7. Акт классификации информационных систем персональных данных.

5. Цели обработки персональных данных.

5.1. Оператор обрабатывает персональные данные исключительно в следующих целях:

5.1.1. Исполнения положений нормативных актов, указанных в п.4.1. настоящей Политики.

5.1.2. Принятие решения о трудоустройстве соискателя.

5.1.3. Заключение и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами.

5.1.4. Предоставления субъектам персональных данных квалифицированной медицинской помощи, учета результатов договорных обязательств, а также наиболее полного исполнения учреждением обязательств и компетенций в соответствии с Федеральным законом "Об обязательном медицинском страховании граждан в Российской Федерации" от 29 ноября 2010 года № 326-ФЗ и Федеральным законом "Об основах охраны здоровья граждан в Российской Федерации" от 21.11.2011 № 323-ФЗ.

5.1.5. Сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача ПД по системе «VipNet» и РМИАС. Обработка персональных данных: смешанная; с передачей по внутренней сети Оператора, с передачей по сети Интернет.

Обработка персональных данных пациентов Оператора осуществляется для решения следующих задач:

- Осуществление расчетов с ФОМС и страховыми организациями за оказание медицинских услуг застрахованным.
- Формирования отчетов по Стоматологической поликлинике.
- Назначение и начисление счетов на оказание услуг и иных выплат.
- Бухгалтерский учет и контроль финансово-хозяйственной деятельности Оператора и исполнения финансовых обязательств по заключенным договорам.
- Обработка амбулаторных карт (в т.ч. в электронной форме).

- Поддержание контактов с законными представителями субъекта персональных данных.
- Проведение лечебно-профилактических мероприятий.
- Иные задачи, необходимые для повышения качества и эффективности деятельности Оператора.

6. Категории обрабатываемых персональных данных

6.1. В информационных системах персональных данных Оператора обрабатываются следующие категории персональных данных:

6.1.1. Персональные данные сотрудников.

6.1.2. Персональные данные кандидатов на замещение вакантных должностей Оператора.

6.1.3. Персональные данные пациентов - лиц, которым оказываются или уже оказаны медицинские услуги специалистами Оператора.

При обращении к Оператору пациент предоставляет следующую информацию:

- ФИО.
- Дата рождения.
- Адрес прописки.
- Адрес фактического проживания.
- Паспортные данные.
- Данные полиса медицинского страхования.
- СНИЛС.
- Рабочее положение, место работы.
- Семейное положение
- Социальная категория.
- Пол.
- Профессия (образование).
- Данные о состоянии здоровья (история болезни, цель посещения, исход лечения и т.д.).

6.1.4. Перечень действий:

- неавтоматизированная обработка - ведение трудовых книжек, личных дел, больничных листов, историй болезней, журналов, договоров;
- автоматизированная обработка - внесение персональных данных в ИСПДн «Сотрудники» и ИСПДн «Пациенты»;

Данная информация собирается исключительно с письменного согласия на обработку персональных данных субъекта персональных данных или его законного представителя. При отказе субъекта персональных данных дать согласие ему объясняются последствия такого отказа.

В соответствии с ст. 7 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Учреждение не раскрывает персональные данные третьим лицам и не распространяет их без согласия субъекта персональных данных.

Субъект персональных данных имеет право на доступ к своим персональным данным по письменному запросу на имя Главного врача. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя

7. Принципы обработки персональных данных

7.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона 152-ФЗ «О персональных данных».

7.2. Оператор не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

7.3. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

8. Сведения о третьих лицах, участвующих в обработке персональных данных

8.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

8.1.1. Федеральной налоговой службе.

8.1.2. Пенсионному фонду Российской Федерации.

8.1.3. Фонду медицинского страхования Российской Федерации.

8.1.4. Кредитным организациям.

8.1.5. Организациям в соответствии с заключенными государственными контрактами на поставку технических средств реабилитации на выполнение работ по обеспечению инвалидов протезно-ортопедическими изделиями.

9. Меры по обеспечению безопасности персональных данных при их обработке

9.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

9.1.1. Назначением ответственных за организацию обработки персональных данных.

9.1.2. Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

9.1.3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.

9.1.4. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

9.1.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

9.1.6. Учетом машинных носителей персональных данных.

9.1.7. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

9.1.8. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.1.9. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

9.1.10. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

9.1.11. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

9.2. Обязанности должностных лиц, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются в «Положении о персональных данных».

10. Права субъектов персональных данных

10.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

10.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

10.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

10.4. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

10.5. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных (см.п.11.2).

10.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

11. Контроль и надзор за обработкой персональных данных

11.1. Ответственным за организацию обработки и обеспечения безопасности персональных данных в Государственном автономном учреждении здравоохранения Республики Башкортостан Стоматологическая Поликлиника № 8 города Уфа назначены: начальник отдела кадров – в части: контроля соблюдения сотрудниками, обрабатывающими персональные данные, организационных условий обеспечения безопасности персональных данных; подготовки и внесения изменений в документы по защите персональных данных; контроля за проведением внутренних проверок, согласно утвержденного Плана мероприятий по внутреннему контролю за соблюдением безопасности персональных данных; в части контроля соблюдения сотрудниками, обрабатывающими персональные данные, технических условий обеспечения безопасности персональных данных; обеспечения штатных режимов работы технических средств обеспечения безопасности персональных данных; организации проведения внутренних проверок, согласно утвержденного Плана мероприятий по внутреннему контролю за соблюдением безопасности персональных данных – программиста;

11.2. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

11.2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

11.3. Управление Роскомнадзора по Республике Башкортостан:

450005, Республика Башкортостан

г. Уфа, ул. 50 лет Октября, д. 20/1

Телефон: (347) 279–11–00

Круглосуточный дежурный телефон (347) 279–11–11

12. Заключительные положения

12.1. Настоящая политика утверждается главным врачом.

12.2. Оператор имеет право вносить изменения в настоящую Политику.

12.3. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения и размещения на сайте Оператора, если иное не предусмотрено новой редакцией Политики.

12.4. Настоящая политика обязательна для соблюдения и ознакомления всех сотрудников Оператора.