

Утверждено
приказом главного врача ГАУЗ «НЦРМБ»
от 21 февраля 2019 года № 08-ОД

**ПОЛИТИКА
ГОСУДАРСТВЕННОГО АВТОНОМНОГО
УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ
«НИЖНЕКАМСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ
МНОГОПРОФИЛЬНАЯ БОЛЬНИЦА»
(ГАУЗ «НЦРМБ»)
В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ
ПЕРСОНАЛЬНЫХ ДАННЫХ
(в редакции от 21.02.2019)**

город Нижнекамск
2019

1. Назначение

1.1. Настоящий документ определяет политику Государственного автономного учреждения здравоохранения «Нижекамская центральная районная многопрофильная больница» (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, субъектов ПДн, обрабатываемых Оператором, а также выполнение 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 гарантированного выполнения норм федерального законодательства Оператор считает важнейшей задачей соблюдение принципов законности, целостности и конфиденциальности при обработке ПДн, 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, а также на подразделения, принимающие участие в указанных процессах.

3. Информация об Операторе

Наименование: Государственное автономное учреждение здравоохранения «Нижнекамская центральная районная многопрофильная больница».

Краткое наименование: ГАУЗ «НЦРМБ».

ИНН 1651064944

КПП 165101001

Фактический адрес: 423570, Республика Татарстан, город Нижнекамск, улица Ахтубинская, дом 9

Телефон/факс: 24-31-70

В реестре операторов персональных данных под регистрационным номером 12-0235780

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. Конституция Российской Федерации.

4.1.2. Трудовой кодекс Российской Федерации.

4.1.3. Гражданский кодекс Российской Федерации.

4.1.4. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

4.1.5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

4.1.6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4.1.7. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.1.8. Постановление Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

4.1.9. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите

персональных данных для каждого из уровней защищенности (утв. Приказом ФСБ России от 10.07.2014 N 378).

4.1.10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14.02.2008 заместителем директора ФСТЭК России).

4.1.11. ФЗ №326 от 29 ноября 2010 года «Об обязательном медицинском страховании в Российской Федерации».

4.1.12. Федеральный закон от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации".

4.1.13. Федеральный закон от 2 мая 2006 г. №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

4.1.14. Закон Республики Татарстан от 22 декабря 2012 года № 87-ЗРТ «О регулировании отдельных вопросов в сфере охраны здоровья граждан в Республике Татарстан».

4.2. Во исполнение настоящей Политики Оператором утверждены следующие локальные нормативные правовые акты:

4.2.1. Положение об обработке и защите персональных данных

4.2.2. Приказ об утверждении перечня информационных систем персональных данных.

4.2.3. Перечень персональных данных, обрабатываемых в информационных системах персональных данных.

4.2.4. Приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

4.2.5. Акт классификации информационных систем персональных данных ГАУЗ «НЦРМБ».

4.2.6. Акт определения уровня защищенности информационных систем персональных данных ГАУЗ «НЦРМБ».

4.2.7. Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных.

4.2.8. Модель нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных.

4.2.9. Приказ об утверждении мест хранения материальных носителей ПДн.

4.2.9. Приказ об утверждении списка должностей, которым необходим доступ к ПДн, обрабатываемым в информационных системах персональных данных, для выполнения служебных (трудовых) обязанностей.

4.2.10. Инструкции пользователя информационных систем персональных данных.

4.2.11. Другие внутренние организационно-распорядительные документы определяющие политику Оператора в области обработки и защиты персональных данных.

5. Цели обработки персональных данных

Оператор обрабатывает персональные данные исключительно в следующих целях, согласно реестру операторов персональных данных:

1. обеспечение исполнения трудовых отношений между работником и работодателем;
2. обеспечение исполнения договора гражданско-правового характера, государственного контракта с физическими лицами, оказывающими услуги Оператору;
3. регистрация сведений, необходимых для установления медицинских диагнозов, оказания медицинских услуг, обработка персональных данных осуществляется в медико-профилактических целях, оказания медицинских и медико-социальных услуг, для статистических и иных научных целей;
4. повышение качества обслуживания в учреждении. Рассмотрение жалоб, обращений и (или) предложений физических лиц написавших сообщения на официальном сайте Оператора, или подавших письменное обращение в адрес Оператора.

6. Категории обрабатываемых персональных данных

6.1. В информационной системе ПДн Оператора обрабатываются следующие категории ПДн:

- 6.1.1. работников, состоящих в трудовых отношениях с Оператором (работодателем) и их иждивенцев;
- 6.1.2. близких родственников работников Оператора;
- 6.1.3. физических лиц, получающих медицинские услуги в учреждении здравоохранения;
- 6.1.4. физических лиц, оказывающих услуги учреждению на основании гражданско-правового договора;
- 6.1.5. физических лиц, подавших жалобу, обращение и (или) предложение в адрес Оператора.

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 производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу)

передачу персональных данных.

7.3. Обработка персональных данных Оператором осуществляется на основе следующих принципов:

7.3.1 Обработка персональных данных осуществляется на законной и справедливой основе;

7.3.2 Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

7.3.3 Обработке подлежат только те персональные данные, которые отвечают целям их обработки;

7.3.4 Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям обработки;

7.3.5 При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.

7.3.6 Сроки хранения персональных данных установлены нормами федерального законодательства, указанных в п.4.1.

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

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

— Управление здравоохранения по Нижнекамскому муниципальному району Министерства здравоохранения Республики Татарстан (Республика Татарстан, г. Нижнекамск, ул. Менделеева, 32А);

— Государственное учреждение «Управление пенсионного фонда РФ в Нижнекамском районе и г. Нижнекамск» (Республика Татарстан, г. Нижнекамск, ул. Мира, 60);

— Государственное казенное учреждение «Центр занятости населения города Нижнекамск» (Республика Татарстан, г. Нижнекамск, ул. Бызова, 20А);

— Общество с ограниченной ответственностью «АК БАРС СТРАХОВАНИЕ» (Республика Татарстан, г. Казань, ул. Меридианная, 1);

— Общество с ограниченной ответственностью страховая медицинская организация «Чулпан-Мед» (Республика Татарстан, г. Альметьевск, ул. Пушкина, 66);

— Межрайонная инспекция Федеральной налоговой службы №11 по Республике Татарстан (Республика Татарстан, г. Нижнекамск, пр. Шинников, 4);

— Территориальное отделение Департамента казначейства МФ РТ Нижнекамского района и города Нижнекамска (Республика Татарстан, г. Нижнекамск, ул. Ахтубинская, 6);

— Акционерный коммерческий банк «АК БАРС» (публичное акционерное общество) (Республика Татарстан, г. Нижнекамск, ул. Баки Урманче, 18);

— Открытое акционерное общество Сбербанк России, Нижнекамское отделение (Республика Татарстан, г. Нижнекамск, пр. Вахитова, 27);

— Управление Федерального казначейства по Республике Татарстан (Республика Татарстан, г. Казань, ул. Вишневого, 31);

— ГАУЗ Республиканский медицинский информационно-аналитический центр (РМИАЦ) (Республика Татарстан, г. Казань, ул. А. Кутуя, 88);

— иным органам и организациям, в случаях и порядке, предусмотренными законодательством РФ.

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. Осуществление внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» 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 работников.

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, в частности, применением средств криптографической защиты информации КристоПро CSP.

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 над 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 об обеспечении безопасности персональных данных» и локально утверждённых специальных инструкциях.

10. Права субъектов персональных данных

10.1. В соответствии с №152-ФЗ «О персональных данных» субъект персональных данных имеет право:

10.1.1. Получить сведения, касающиеся обработки ПДн оператором, а именно:

- 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 №152-ФЗ «О персональных данных»;

- информацию об осуществленной или 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 №152-ФЗ «О персональных данных» или другими федеральными законами.

10.1.2. Потребовать от оператора 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.

10.1.3. Заявить возражение против принятия в отношении себя решений, порождающих юридические последствия на основе исключительно автоматизированной обработки персональных данных.

10.1.4. Отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

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

10.3. Для реализации своих прав (см. пп. 10.1.1–10.1.4.) 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.

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

10.5. 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 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.

12. Заключительные положения

12.1. Оператор имеет право вносить изменения в настоящую Политику.

12.2. 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.