

УТВЕРЖДАЮ

Главный врач

ГБУЗ СО «Кинель-Черкасская ЦРБ»

Н.Г. Нугманов



» 14 января 2019

Политика

**в отношении обработки персональных данных
государственного бюджетного учреждения Самарской области
«Кинель-Черкасская центральная районная больница»**

1. Общие положения

- 1.1. Настоящая политика в отношении обработки персональных данных (далее политика) действует в отношении всей информации, которую ГБУЗ СО «Кинель-Черкасская ЦРБ (далее – Учреждение) может получить о физических лицах в рамках осуществления своей деятельности. Политика определяет основные цели, задачи, общие принципы и направления обеспечения надлежащей обработки персональных данных Учреждения и предназначена для ознакомления неограниченного круга лиц.
- 1.2. Политика обязательна для исполнения всеми лицами, непосредственно осуществляющими обработку персональных данных в Учреждении.
- 1.3. Все персональные данные в Учреждении, за исключением обезличенных и сделанными общедоступными субъектом персональных данных, признаются информацией ограниченного доступа. Необходимость соблюдения конфиденциальности такой информации определена требованиями Федерального закона «О персональных данных».
- 1.4. Политика подлежит пересмотру в ходе периодического анализа со стороны руководства Учреждения, а также в случаях изменения законодательства Российской Федерации в области персональных данных.
- 1.5. Политика подлежит опубликованию на официальном сайте Учреждения.
- 1.6. Учреждение осуществляет обработку персональных данных на основании:
 - Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
 - Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Принципы обработки персональных данных

- 2.1. Осуществление обработки персональных данных на законной и справедливой основе.
- 2.2. Соответствия целей обработки персональных данных полномочиям Учреждения.
- 2.3. Соответствие содержания и объема обрабатываемых персональных данных целям обработки персональных данных.
- 2.4. Достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных.
- 2.5. Ограничение обработки персональных данных при достижении конкретных и законных целей, запрет обработки персональных данных, несовместимых с целями сбора персональных данных.
- 2.6. Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- 2.7. Осуществление хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3. Цели обработки персональных данных

- 3.1. Учреждение обрабатывает персональные данные для оказания медицинских услуг и осуществления административно-хозяйственной деятельности.

3.2. Учреждение осуществляет обработку персональных данных сотрудников в следующих целях:

- для ведения кадрового учета сотрудников Учреждения;
- для подбора сотрудников Учреждения;
- для ведения налоговой отчетности и осуществления взаиморасчетов с сотрудниками Учреждения;
- для направления сотрудников Учреждения в командировки;
- для ведения локальных/общедоступных справочников сотрудников Учреждения.

3.3. Учреждение осуществляет обработку персональных данных контрагентов в следующих целях:

- для заключения договоров с контрагентами.

3.4. Учреждение осуществляет обработку персональных данных пациентов в следующих целях:

- для оказания медицинских услуг;
- для формирования медицинской карты пациента (в т.ч. в электронном виде);
- для ведения персонифицированного учета в сфере обязательного медицинского страхования в соответствии с действующим законодательством;
- для ведения отчетности;
- для принятия решений по обращениям граждан Российской Федерации в соответствии с законодательство.

4. Правила обработки персональных данных

4.1. В учреждении осуществляется обработка персональных данных следующих категорий субъектов:

- сотрудников Учреждения;
- контрагентов (физические лица и представители юридических лиц);
- пациентов Учреждения для оказания им медицинских услуг по ОМС;
- пациентов Учреждения для оказания им платных медицинских

услуг на договорной основе;

- иных лиц, давших согласие Учреждению, как оператору, на обработку своих персональных данных, либо сделавших общедоступными свои персональные данные, а так же в других случаях, предусмотренных законодательством Российской Федерации.

4.2. В учреждении назначается лицо, ответственное за организацию обработки и обеспечение безопасности персональных данных (далее - Ответственное лицо).

4.3. Решения об инициации новых процессов обработки персональных данных или внесении изменений в существующие процессы обработки персональных данных согласовываются с Ответственным лицом.

4.4. Доступ к персональным данным имеют сотрудники Учреждения, которые обязаны осуществлять их обработку в связи с исполнением ими должностных обязанностей. Перечень структурных подразделений и сотрудников, участвующих в обработке персональных данных, определяется Ответственным лицом.

4.5. Обработка персональных данных в Учреждении осуществляется с использованием и без использования средств автоматизации.

5. Перечень действий с персональными данными

Учреждение осуществляет обработку (сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе и передачу), обезличивание, блокирование, уничтожение персональных данных с использованием средств автоматизации, а так же без использования таких средств. Учреждение может передавать персональные данные третьим лицам в случаях, если:

- субъект дал согласие на осуществление таких действий;
- это необходимо для осуществления и выполнения возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей;

- в других случаях, предусмотренных законодательством Российской Федерации.

Трансграничная передача персональных данных не осуществляется.

6. Права субъектов персональных данных

6.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

6.2. Обязанность предоставить доказательство получения субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в Федеральном законе «О персональных данных» возлагается на Учреждение.

6.3. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающим его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

6.4. Субъект персональных данных имеет право:

- получить у Учреждения информацию, которая касается обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами;
- принимать предусмотренные законом меры по защите своих прав и требовать от Учреждения уточнения его персональных данных, а также их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. В таком случае

Учреждение обязано немедленно прекратить по требованию субъекта обработку персональных данных;

- обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Организация защиты персональных данных

7.1. Защита персональных данных от неправомерного или случайного доступа, уничтожения. Изменения, блокирования, предоставления и распространения, а также от иных неправомерных действий обеспечивается Учреждением. В отдельных случаях для выполнения части функций по обеспечению безопасности персональных данных Учреждения могут привлекаться сторонние организации, имеющие оформленные в установленном порядке лицензии на осуществление деятельности по технической защите конфиденциальной информации.

7.2. Защите подлежат все обрабатываемые в Учреждении персональные данные, за исключением обезличенных персональных данных и персональных данных, сделанных общедоступными субъектом.

7.3. Общую организацию защиты персональных данных субъектов и контроль над соблюдением сотрудниками Учреждения мер и мероприятий по защите персональных данных осуществляет ответственное лицо.

7.4. Меры, принимаемые для защиты персональных данных субъектов персональных данных:

- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями действующего

законодательства о персональных данных, требованиям к защите персональных данных и иными документами по вопросам обработки персональных данных;

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- осуществление учета машинных носителей персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- разработка локальных документов по вопросам обработки персональных данных;
- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;

- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

8. Условия прекращения обработки персональных данных

- 8.1. Срок или условие прекращения персональных данных работников в Учреждении – 75 лет.
- 8.2. Срок или условие прекращения персональных данных контрагентов в Учреждении – по исполнению обязательств по договору и в течении срока исковой давности.
- 8.3. Срок или условие прекращения обработки персональных данных пациентов в Учреждении составляет 25 лет для медицинских карт стационарных больных и 5 лет для медицинских карт амбулаторных больных.

9. Изменение политики

Учреждение имеет право вносить изменения в настоящую Политику.

При внесении изменений в заголовке Политики указывается дата последнего обновления редакции.