

УТВЕРЖДАЮ
Главный врач
ООО «Улыбнись!»

О.Е. Левцанова

« 18 »



2017 г.

**ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ООО «Улыбнись!»**

1. Введение.
2. Общие положения.
3. Основные понятия, используемые в настоящем документе.
4. Обрабатываемые персональные данные.
5. Цели сбора и обработки персональных данных.
6. Условия обработки персональных данных и их передача третьим лицам.
7. Защита персональных данных.
8. Основные права и обязанности субъекта персональных данных и оператора в сфере обработки персональных данных.
9. Ответственность.

1. ВВЕДЕНИЕ

Настоящим документом определяется политика ООО «Улыбнись!» (далее по тексту – клиника) в отношении обработки персональных данных (далее по тексту - ПД).

Документ предназначен для ознакомления неограниченного круга лиц.

Политика разработана в соответствии с действующим законодательством Российской Федерации о ПД:

- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства Российской Федерации от 15.09.2008 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Действие настоящей Политики распространяется на любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ) обезличивание, блокирование, удаление, уничтожение ПД.

Настоящая Политика подлежит пересмотру и, при необходимости, актуализации в случае изменений в законодательстве Российской Федерации о ПД.

2. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ДОКУМЕНТЕ

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация,

определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений и здравоохранения.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке и действия (операции) совершаемые с персональными данными.

Обработка персональных данных - действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, комбинирование, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые клиници в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки

персональных данных и обеспечение организационно-технических мер защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения.

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

3. ОБЩИЕ ПОЛОЖЕНИЯ

Целью Политики клиники в отношении обработки персональных данных является обеспечение безопасности, 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.

Политика клиники в отношении обработки персональных данных направлена на защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обработка персональных данных в клинике осуществляется на основе следующих принципов:

- соблюдение законности и справедливости обработки ПД;
- недопущение обработки персональных данных, несовместимых с целями сбора персональных данных, предусмотренных настоящей Политикой;
- базы данных, содержащие персональные данные, обработка которых осуществляется в несовместимых между собой целях, объединению не подлежат;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки.
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.
- обеспечение принятия необходимых мер по удалению или уточнению неполных или неточных персональных данных.
- соблюдение законности по уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.
- соблюдение прав субъекта персональных данных на доступ к его персональным данным.

Клиника не производит обработку персональных данных субъектов персональных данных в целях политической агитации.

4. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Информационные системы персональных данных, принадлежащие **клинике**, предназначены для обработки персональных данных следующих категорий субъектов персональных данных:

- физических лиц, состоящих в трудовых отношениях с клиникой, в том числе бывших сотрудников по срочному, бессрочному трудовому или гражданско-правовому договорам;
- физических лиц, обратившихся за медицинской помощью в клинику;
- физических лиц, являющихся кандидатами на работу;
- физических лиц, являющихся близкими родственниками сотрудников учреждения;
- физических лиц, которым оказывается медицинская помощь в клинике на основании соответствующего договора.

5. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели обработки персональных данных в клинике определены в соответствии с действующим законодательством и Уставом клиники.

Основными целями обработки персональных данных являются:

- обеспечение организации оказания медицинской помощи населению, наиболее полного исполнения обязательств и компетенций в соответствии с Федеральным законом от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 12.04.2010 N 61-ФЗ «Об обращении лекарственных средств»;
- осуществление трудовых отношений, исполнение обязанностей работодателя в соответствии с требованиями законодательства Российской Федерации: трудоустройстве работников; ведении кадрового делопроизводства; обеспечении личной безопасности работников; контроле количества и качества выполняемой работы; обеспечения сохранности имущества; охраны труда;
- исполнение гражданско-правовых договоров, стороной которых, является субъект персональных данных;
- осуществление иных видов деятельности для достижения основных целей, предусмотренных Уставом **клиники**.

6. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ПЕРЕДАЧА ТРЕТЬИМ ЛИЦАМ

Обработка персональных данных в клинике осуществляется неавтоматизированным и автоматизированным способом.

К обработке персональных данных в клинике допускаются только сотрудники, прошедшие определенную процедуру допуска, к которой относятся:

- надлежащее ознакомление (под роспись) сотрудников с локальными нормативными актами клиники, регламентирующими порядок работы с персональными данными;

- дача сотрудником подписки о соблюдении конфиденциальности и неразглашении сведения при работе с персональными данными;

- получение сотрудником и использование в работе индивидуального доступа к информационным системам, содержащим персональные данные.

Сотруднику, осуществляющему функции по обработке персональных данных выдаются только необходимые для исполнения обязанностей права на доступ в информационные системы персональных данных.

Сотрудники, имеющие доступ к персональным данным, получают только те персональные данные, которые необходимы им для выполнения конкретных обязанностей.

Хранение персональных данных осуществляется в бумажном и электронном виде.

Персональные данные могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

Персональные данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях хранятся в разных папках (вкладках).

Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в информационной системе персональных данных. Хранение персональных данных в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем это требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок.

Для уничтожения бумажных документов допускается применение shreddera.

Персональные данные, хранение которых осуществляется на электронном носителе, уничтожаются путем стирания, форматирования или уничтожения носителя.

Уничтожение ПД производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении путем стирания форматирования или уничтожения носителей, подписанным членами комиссии.

Передача персональных данных осуществляется клиникой осуществляется исключительно в целях обработки персональных данных.

Передача персональных данных осуществляется в случае если:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена действующим законодательством в порядке, предусмотренном законодательством при точном соблюдении законности по обеспечению конфиденциальности и безопасности полученных сведений.

Предоставление сведений, составляющих врачебную тайну, без согласия пациента или его законного представителя допускается в случаях, предусмотренных действующим законодательством, в том числе:

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;
- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

При обработке персональных данных клиника принимает на себя обязательства по принятию необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных в клинике достигается следующими мерами:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает, установленные Правительством Российской Федерации уровни защищенности ПД;

- применение прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации средств защиты информации для нейтрализации актуальных угроз безопасности;

- оценка эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию информационной системы ПД;

- учет машинных носителей ПД;

- обнаружение фактов несанкционированного доступа к ПД и принятие мер по их нейтрализации;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- определением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

- назначением сотрудника, ответственного за организацию обработки ПД;

- назначение структурного подразделения, ответственного за обеспечение безопасности персональных данных;

- определением списка лиц, допущенных к работе с ПД;

- разработкой и утверждением локальных нормативных актов клиники, регламентирующих порядок обработки ПД;

- контроль соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, локальным актам клиники, в том числе контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

- ответственность за нарушение установленных правил обработки ПД.

8. ОСНОВНЫЕ ПРАВА, ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПЕРАТОРА В СФЕРЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»

Субъект персональных данных вправе требовать 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, а также принимать предусмотренные законом меры по защите своих прав.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) 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;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в случаях, предусмотренных действующим законодательством.

Субъект персональных данных вправе требовать 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, а также принимать предусмотренные законом меры по защите своих прав.

Сведения, касающиеся обработки персональных данных субъекта, должны быть предоставлены субъекту персональных данных клинике в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Субъекту или его представителю клиника должна быть предоставлена информация о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также должна быть предоставлена возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

Порядок обработки запросов субъектов персональных данных по соблюдению их законных прав в **клинике** осуществляется в соответствии с действующим законодательством в области защиты персональных данных.

Клиника обязуется осуществлять обработку персональных данных только с согласия субъектов персональных данных, за исключением случаев, предусмотренных Федеральным №152-ФЗ «О персональных данных».

Клиника обязано отвечать на запросы субъектов персональных данных, их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в соответствии с требованиями законодательства.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Клиника обязуется уведомлять уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

9. ОТВЕТСТВЕННОСТЬ

Клиника несет ответственность за нарушение требований законодательства, регулирующего правоотношения в сфере обработки персональных данных в соответствии с действующим законодательством Российской Федерации.

Вопросы, касающиеся обработки персональных данных, не урегулированные настоящим документом, разрешаются в неукоснительном соответствии с нормами и требованиями законодательства указанной сферы правоотношений.