

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ ООО «ДАНТИСТ»

1. Общие положения

1.1. Политика обработки персональных данных в ООО «Дантист» (далее — Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, функции ООО «Дантист» при обработке персональных данных, права субъектов персональных данных, а также реализуемые в ООО «Дантист» требования к защите персональных данных.

1.2. Политика разработана в соответствии с п.2 ст.18.1 Федерального закона № 152 -ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом медицинской организации ООО «Дантист» (далее Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Организация.

1.3. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.4. Положение Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.5. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в ООО «Дантист» вопросы обработки персональных данных работников.

2. Законодательные и иные нормативные правовые акты Российской Федерации, в соответствии с которыми определяется Политика обработки персональных данных в ООО «Дантист»

2.1. Политика обработки персональных данных в ООО «Дантист» определяется в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Федерации и нормативные документы уполномоченных органов государственной власти.

Кроме того обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 12 Трудового кодекса), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

2.2. В целях реализации положений Политики в ООО «Дантист» разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

- Положение об обработке персональных данных в ООО «Дантист»;
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Дантист»;
- иные локальные нормативные акты и документы, регламентирующие в ООО «Дантист» вопросы обработки персональных данных.

2.3. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

2.4. Действующая редакция хранится в месте нахождения Организации по адресу: город Качканар, улица Свердлова, дом 23, пом.1-5. Электронная версия Политики на сайте: www.dentistkch.ru

3. Термины и принятые сокращения

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения — персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном действующим законодательством Российской Федерации.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемые 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.

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

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, когда 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 становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных — 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.

Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий.

Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

4. Принципы обеспечения безопасности персональных данных

4.1. ООО «Дантист», являясь оператором персональных данных, осуществляет обработку персональных данных субъектов персональных данных, состоящих с ООО «Дантист» в договорных отношениях.

4.2. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно - технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

4.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

– законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

– системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

– комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4.3. В организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено Федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаться или обезличиваются.

4.4. При обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. ООО «Дантист» принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных ПДн;

- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Персональные данные обрабатываются в ООО «Дантист» в целях:

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов ООО «Дантист»;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на ООО «Дантист», в том числе по предоставлению персональных данных в органы государственной власти;
- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
- подготовки, заключения, исполнения и прекращения договоров;
- формирования справочных материалов для внутреннего информационного обеспечения деятельности ООО «Дантист»,
- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- осуществления прав и законных интересов ООО «Дантист» в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами ООО «Дантист», или третьих лиц либо достижения общественно значимых целей;
- в иных законных целях.

5.1. При обработке все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

5.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

6. Перечень субъектов, персональные данные которых обрабатываются в ООО «Дантист»

В ООО «Дантист» обрабатываются персональные данные следующих категорий субъектов:

- потребители (пациенты) услуг ООО «Дантист»;
- законные представители потребителей (пациенты) услуг ООО «Дантист»;
- работники ООО «Дантист».

7. Перечень персональных данных, обрабатываемых в ООО «Дантист»

7.1. Перечень персональных данных, обрабатываемых в ООО «Дантист»:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи;
- сведения о трудовом стаже;
- СНИЛС;
- ИНН;
- фотографии, другие данные, которые добровольно предоставили в порядке заключения договора, обучения, анкетирования, при опросах.

Обработка биометрических персональных данных с целью идентификации в ООО «Дантист» не осуществляется.

7.2. Документы, содержащие ПДн создаются путем:

- а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- б) внесения сведений в учетные формы;
- в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

7.3. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

7.4. Цели обработки ПДн:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

7.5. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

7.6. ПДн, обрабатываемые Организацией:

- данные полученные при осуществлении трудовых отношений;
- данные полученные для осуществления отбора кандидатов на работу в организацию;
- данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оказании медицинской помощи.

Полный список ПДн представлен в Перечне ПДн, утвержденном главным врачом Организации.

7.7. Перечень действий с персональными данными и способы их обработки:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление и уничтожение персональных данных.

7.8. Обработка персональных данных ведется:

– с использованием средств автоматизации.

7.9. Хранение ПДн

7.9.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

7.9.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа (регистратура).

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

7.9.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

7.9.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

7.9.6. Хранение персональных данных осуществляется на электронных носителях и/или в бумажном варианте на неограниченный срок.

7.10. Уничтожение ПДн

7.10.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

7.10.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

7.10.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

7.11. Передача ПДн

7.11.1. Организация передает ПДн третьим лицам в следующих случаях:

– субъект выразил свое согласие на такие действия;

– передача информации, содержащей сведения о персональных данных по телефону, факсу, электронной почте и бумажных носителях без письменного согласия лица запрещается;

– передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

7.12. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические фирмы, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

8. Защита персональных данных

8.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

8.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

8.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

8.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

8.5. Основными мерами защиты ПДн, используемыми Организацией, являются:

8.5.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;

8.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;

8.5.3. Разработка политики в отношении обработки персональных данных;

8.5.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПД;

8.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

- 8.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;
- 8.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- 8.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;
- 8.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;
- 8.5.10. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн
- 8.5.11. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
- 8.5.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8.5.13. Обучение работников Организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
- 8.5.14. Осуществление внутреннего контроля и аудита.

9. Основные права субъекта ПДн и обязанности Организации

9.1. Основные права субъекта ПДн

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

- 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 Федеральным законом «О персональных данных»;
- информацию об осуществленной или о 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 настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн 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.

9.2. Обязанности Организации

Организация обязана:

– при сборе ПДн предоставить информацию об обработке его ПДн;

– в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;

– при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;

– давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.