

Политика в отношении обработки персональных данных стоматологической клиники «Корона»

1. Общие положения

1.1. Настоящая Политика определяет порядок и условия обработки персональных данных в стоматологической клинике «Корона» (далее — Оператор).

1.2. Политика разработана в соответствии с требованиями действующего законодательства Российской Федерации в области защиты персональных данных и здравоохранения, включая федеральные законы, постановления Правительства РФ и приказы уполномоченных федеральных органов исполнительной власти.

1.3. Политика является общедоступной и распространяется на пациентов, посетителей сайта, сотрудников и иных субъектов персональных данных.

1.4. Оператор обеспечивает защиту персональных данных, связанных с оказанием стоматологических услуг: диагностической, терапевтической, ортопедической, хирургической, имплантологической и ортодонтической деятельности.

1.5. Персональные данные обрабатываются как в автоматизированной, так и в неавтоматизированной формах.

2. Сведения об операторе

2.1. Оператор: ИП Эреджепов Селим Рамазанович, ИНН 910215675205, Симферополь, ул. Глиники, 66Б

2.2. Места хранения медицинских данных расположены по указанному адресу.

2.3. Ответственный за обработку персональных данных: ИП Эреджепов Селим Рамазанович (тел. +7 (978) 038 55 58, korona.clinic@yandex.ru).

3. Правовые основания обработки персональных данных

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ — применяется исключительно в отношении персональных данных сотрудников Клиники и не распространяется на пациентов и посетителей сайта. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан»;

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

приказ Министерства здравоохранения РФ от 04.03.2019 № 110н «Об обработке персональных данных в Министерстве здравоохранения Российской Федерации»,

приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

приказ ФСБ России от 10.07.2014 № 378 " Об утверждении Состав и содержания 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».

4. Цели обработки персональных данных

Обработка персональных данных осуществляется в следующих целях:

4.1. Оказание стоматологических услуг, включая диагностику (осмотр, КТ, ОПТГ, рентген, 3D-сканирование), лечение, анестезию, хирургические вмешательства, протезирование, ортодонтическое лечение — на основании пункта 5 части 1 статьи 6 Федерального закона №152-ФЗ (необходимость для исполнения договора с субъектом ПДн) и п. 3, п. 4 ч. 2 ст. 10 того же закона (медицинские цели, врачебная тайна).

4.2. Ведение медицинской документации, включая формирование и хранение медицинских карт, электронных записей, рентгенологического архива, стоматологических моделей и 3D-сканов — в соответствии с требованиями Федерального закона №323-ФЗ и нормативных актов Минздрава России (в т. ч. Приказ №1 10 н).

4.3. Исполнение договоров, в том числе по программам добровольного медицинского страхования (ДМС), — на основании пункта 5 части 1 статьи 6 ФЗ-152.

4.4. Исполнение обязанностей, возложенных законодательством Российской Федерации, включая предоставление информации государственному и надзорным органам — на основании пункта 2 части 1 статьи 6 ФЗ-152.

4.5. Ведение кадрового и бухгалтерского учёта — в отношении сотрудников Клиники, на основании трудового и налогового законодательства РФ (пункт 2 части 1 статьи 6 ФЗ-152 и Трудовой кодекс РФ).

4.6. Обеспечение санитарно-эпидемиологического благополучия и соблюдение требований санитарного законодательства — на основании пункта 2 части 1 статьи 6 ФЗ-152.

4.7. Обработка персональных данных, полученных через официальный сайт «Корона», в целях:

 обратной связи с Пользователем,
 записи на приём,
 информирования о деятельности Клиники (в том числе об услугах и изменениях в расписании), на основании согласия субъекта персональных данных (пункт 1 части 1 статьи 6 Ф 3-152), за исключением случаев, когда обработка необходима для ответа на запрос пользователя.

4.8. Информирование пациентов и посетителей сайта об акциях, новых услугах и мероприятиях Клиники — на основании согласия субъекта персональных данных.

4.9. Проведение маркетинговых и статистических исследований — в обезличенном виде, либо с согласия субъекта персональных данных (в случае обработки идентифицируемых данных).

5. Перечень обрабатываемых персональных данных

5.1. Общие персональные данные: ФИО, дата рождения, адрес, контактная информация, паспортные данные, сведения о законных представителях.

5.2. Медицинские персональные данные: диагнозы, стоматологический статус, рентген-снимки, КТ, ОПТГ, данные анамнеза, сведения об аллергиях, ортопедические модели, 3D-сканы, иные сведения, необходимые для лечения. Сведения о состоянии здоровья, предоставляемые через формы сайта (включая текстовые описания симптомов, фотографии, изображения зубов), относятся к специальным категориям персональных данных в соответствии со ст. 10 ФЗ-152 и обрабатываются только при наличии отдельного согласия.

5.3. Биометрические персональные данные (3D-сканы лица/челюстей, цифровые модели, фотограмметрические данные, используемые для идентификации личности) обрабатываются только при наличии отдельного письменного согласия пациента, оформленного в порядке, установленном законодательством Российской Федерации и Приказом Минздрава России №110н.

5.4. Персональные данные, полученные через сайт без заключения договора: имя, номер телефона, адрес электронной почты, ГР-адрес, данные браузера, аналитическая информация (в случае идентификации пользователя).

6. Источники получения персональных данных

Персональные данные могут быть получены Оператором из следующих источников:

- непосредственно от пациента при личном обращении в клинику;
- от законного представителя пациента (в случае лечения несовершеннолетних или недееспособных лиц);

от страховых организаций при оказании услуг по ДМС — в объеме, необходимом для исполнения договора;
из государственных информационных систем — в случаях, прямо предусмотренных законодательством;
через официальный сайт Оператора, включая:

формы онлайн-записи на приём,
формы обратной связи, чат-виджеты и сервисы коммуникации, сбор данных посредством файлов cookie и технических журналов сервера (IP-адрес, дата и время обращения, данные браузера),
аналитические сервисы (например, веб-аналитика), если они используются и позволяют идентифицировать пользователя.

7. Согласие на обработку данных

7.1. Согласие на обработку персональных данных оформляется в письменной форме.

7.2. Согласие на обработку медицинских данных оформляется в соответствии с Приказом Минздрава России № 110 н.

7.3. Информированное добровольное согласие на медицинское вмешательство не заменяет согласия на обработку персональных данных.

8. Передача персональных данных третьим лицам

Передача допускается:

медицинским организациям и лабораториям;
страховым компаниям (ДМС);
зуботехническим лабораториям;
государственным органам по закону;
лицам, осуществляющим порученную обработку (IT-аутсорсеры, хостинг, сервисы рассылок) при условии заключения договора по ст. 6 ФЗ-152 и

соблюдения ими мер защиты. — операторам сотовой связи — исключительно для доставки SMS-уведомлений о записи и приёме, при условии соблюдения требований Ф3-152.

9. Трансграничная передача

9.1. Трансграничная передача не осуществляется, кроме случаев, предусмотренных законодательством и обеспечивающих достаточную защиту.

9.2. Передача медицинских данных без согласия пациента допускается только в случаях, указанных в п.4 ст. 13 Ф3-323.

10. Сроки хранения персональных данных

10.1. Медицинские карты пациентов — 25 лет.

10.2. Рентген-снимки — не менее 5 лет.

10.3. Кадровые документы — 50/75 лет.

10.4. 3D-сканы, цифровые модели — в течение срока лечения и 25 лет (по аналогии с медкартой).

10.5. Персональные данные, полученные через сайт при отсутствии заключения договора на оказание медицинских услуг, хранятся в течение 36 месяцев с даты последнего обращения и подлежат обезличиванию или уничтожению по истечении указанного срока.

10.6. Уничтожение данных осуществляется только при отсутствии обязательных оснований для хранения.

11. Меры по защите персональных данных

Оператор принимает меры, предусмотренные Постановлением № 1119, приказами ФСТЭК и ФСБ:

- разграничение доступа;
- контроль и аудит безопасности;
- антивирусная защита;
- резервное копирование;
- шифрование при передаче медданных;
- защита помещений и серверов;
- обучение персонала.

Уровень защищенности ИСПДн определяется по результатам категорирования.

12. Права субъектов персональных данных

Пациент в праве:

- получать информацию об обработке;
- требовать уточнения или блокирования данных;
- отзывать согласие на обработку персональных данных, за исключением случаев, когда обработка необходима для исполнения договора, оказания медицинской помощи, соблюдения требований законодательства или защиты жизненно важных интересов субъекта;
- получать копии медицинских документов;
- ограничивать обработку;
- обжаловать действия Оператора.

13. Реализация прав субъектов персональных данных

Обращения подаются лично, по почте или в электронной форме с ЭП. Срок рассмотрения — 30 дней. При отказе Оператор предоставляет мотивированный ответ.

14. Действия при инцидентах

При выявлении нарушения безопасности Оператор:

- блокирует доступ;

- проводит расследование;

- уведомляет Роскомнадзор в течение 24 часов;

- уведомляет пациентов, если есть риск нарушения их прав.

15. Изменение Политики

15.1. Политика обновляется при изменении законодательства и технологий обработки.