

УТВЕРЖДАЮ:

Директор

ООО «МЕДЖИКДЕНТ»

(приказ № 2 от 01.06.2025г.)

Магакян А.О. Магакян

«01» июня 2025г.

ПОЛОЖЕНИЕ

О порядке хранения персональных данных работников, клиентов (пациентов) и контрагентов ООО «МЕДЖИКДЕНТ»

1. Термины и определения

Компьютерная программа для стоматологии — медицинская информационная система (МИС), предназначенная для автоматизации работы стоматологических клиник. Она позволяет вести учет пациентов, планировать приемы, вести электронные медицинские карты, контролировать финансовые операции и многое другое. Под МИС в Положении понимается, МИС, расположенная в локальной сети организации по адресу: IDENT-IT.RU. Для работы с персональными данными работников клиники под компьютерной программой для стоматологии в Положении понимается, облачный сервис от фирмы «1С» - 1С:Fresh / 1С: Фреш, позволяющий работать с программами 1С через интернет, а так же комплексное программное обеспечение Saby / СБИС (компания ООО Компания «Тензор»), включающим в себя инструменты для электронной отчетности, документооборота, управления продажами и другими аспектами бизнес-деятельности стоматологии.

Работник, Клиент (пациент) / Контрагент — работник клиники, клиент (пациент клиники) / контрагент (физическое или юридическое лицо), с которым оператор осуществляет свою договорную хозяйственную деятельность в МИС IDENT.

Федеральный закон (ФЗ) — Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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

Оператор — организация, самостоятельно или совместно с другими лицами организующая обработку персональных данных, а также определяющая цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором является общество с ограниченной ответственностью «МЕДЖИКДЕНТ», расположенное по адресу: 354000, Краснодарский край, город-курорт Сочи, ул. Юных Ленинцев, д. 10, помещения 6-9П.

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

Распространение персональных данных — действие, направленное на раскрытие персональных данных определенному кругу лиц по предварительному согласию, в случаях, предусмотренных законом.

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

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если 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 к конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Общие положения

2.1. Положение о порядке хранения персональных данных работников, клиентов (пациентов) и контрагентов (далее — Положение) разработано с целью соблюдения требований законодательства РФ, содержащих персональные данные и идентификации клиентов и контрагентов, находящихся в МИС IDENT, 1С: Фреш, СБИС.

2.2. Положение разработано в соответствии с Конституцией РФ, Гражданским кодексом РФ, действующим законодательством РФ в области защиты персональных данных. Оператор обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

2.3. Положение устанавливает порядок обработки персональных данных работников, клиентов (пациентов) и контрагентов МИС IDENT, 1С: Фреш, СБИС: действия по сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению), уничтожению персональных данных.

2.4. Положение устанавливает обязательные для сотрудников Оператора, задействованных в обслуживании МИС IDENT, 1С: Фреш, СБИС, общие требования и правила по работе со всеми видами носителей информации, содержащими персональные данные работников, клиентов (пациентов) и контрагентов.

2.5. В Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну Российской Федерации.

2.6. Целями Положения являются:

- обеспечение требований защиты прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- исключение несанкционированных действий сотрудников Оператора и любых третьих лиц по сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению) персональных данных, иных форм незаконного вмешательства в информационные ресурсы и локальную вычислительную сеть Оператора, обеспечение правового и нормативного режима конфиденциальности недokumentированной информации работников, клиентов (пациентов) и контрагентов МИС IDENT, 1С: Фреш, СБИС;
- защита конституционных прав граждан на личную тайну, конфиденциальность сведений, составляющих персональные данные, и предотвращение возникновения возможной угрозы безопасности работников, клиентов (пациентов) и контрагентов МИС IDENT, 1С: Фреш, СБИС.

2.7. Принципы обработки персональных данных:

- обработка персональных данных должна осуществляться на законной и справедливой основе;

- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом, договором, стороной которого является работник, клиент (пациент) или контрагент;
- 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.

2.8. Условия обработки персональных данных.

2.8.1. Обработка персональных данных работников, клиентов (пациентов) и контрагентов МИС IDENT, 1С: Фреш, СБИС осуществляется на основании Гражданского кодекса РФ, Конституции РФ, действующего законодательства РФ в области защиты персональных данных.

2.8.2. Обработка персональных данных в МИС IDENT, 1С: Фреш, СБИС осуществляется с соблюдением принципов и правил, предусмотренных Положением и законодательством РФ.

2.9. Цели обработки персональных данных.

2.9.1. Обработка персональных данных работников клиентов (пациентов) и контрагентов МИС IDENT, 1С: Фреш, СБИС осуществляется в целях заключения и/или исполнения договора между работником/клиентом(пациентом)/контрагентом и Оператором.

2.10. Источники получения персональных данных работников, клиентов (пациентов) контрагентов.

2.10.1. Источником информации обо всех персональных данных работника клиента (пациента) контрагента является непосредственно сам работник/клиент(пациент)/контрагент.

2.10.2. Источником информации о персональных данных работника/клиента(пациента)/контрагента являются сведения, полученные вследствие внесения работника/клиента(пациента)/контрагента своих данных в учетные формы.

2.10.3. Персональные данные работника/клиента(пациента)/контрагента относятся к конфиденциальной информации ограниченного доступа.

2.10.4. Обеспечения конфиденциальности персональных данных не требуется в случае их обезличивания, а также в отношении общедоступных персональных данных.

2.10.5. Оператор не имеет права собирать и обрабатывать персональные данные работника/клиента(пациента)/контрагента о его расовой, национальной принадлежности,

политических взглядах, религиозных или философских убеждениях, частной жизни, за исключением случаев, предусмотренных действующим законодательством.

2.10.6. Оператор не имеет права получать и обрабатывать персональные данные работника/клиента(пациента)/контрагента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом.

2.11. Способы обработки персональных данных.

2.11.1. Персональные данные работников/клиентов(клиентов)/контрагентов обрабатываются исключительно с использованием средств автоматизации, а так же без использования средств автоматизации путем хранения в архиве на бумажном носителе медицинских карт клиентов, личных дел сотрудников.

2.12. Права субъектов (работников/клиентов(пациентов)/контрагентов) персональных данных.

2.12.1. Работник/клиент(пациент)/контрагент имеет право на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к конкретному субъекту персональных данных (Работнику/клиенту(пациенту)/контрагенту), а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона «О персональных данных».

2.12.2. Работник/клиент(пациент)/контрагент имеет право на получение от Оператора при личном обращении к нему либо при получении Оператором письменного запроса от работника/клиента(пациента)/контрагента следующей информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором, а также цель такой обработки;
- 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 предоставления 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;
- 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 Федеральным законом или другими федеральными законами;
- требовать изменения, уточнения, уничтожения информации о самом себе;
- обжаловать неправомерные действия или бездействие по обработке персональных данных и требовать соответствующей компенсации в суде;

- на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения;
- определять представителей для защиты своих персональных данных;
- требовать от Оператора уведомления обо всех произведенных в них изменениях или исключениях из них.

2.12.3. Работник/клиент(пациент)/контрагент имеет право обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке действия или бездействие Оператора, если считает, что последний осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы.

2.12.4. Работник/клиент(пациент)/контрагент 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.

2.13. Обязанности Оператора.

2.13.1. По факту личного обращения либо при получении письменного запроса субъекта персональных данных или его представителя Оператор, при наличии оснований, обязан в течение 30 дней с даты обращения либо получения запроса субъекта персональных данных или его представителя предоставить сведения в объеме, установленном Федеральным законом. Такие сведения должны быть предоставлены субъекту персональных данных 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.

2.13.2. Все обращения субъектов персональных данных или их представителей регистрируются в Журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

2.13.3. В случае отказа в предоставлении субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя информации о наличии персональных данных о соответствующем субъекте персональных данных Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных или его представителя, либо с даты получения запроса субъекта персональных данных или его представителя.

2.13.4. В случае получения запроса от уполномоченного органа по защите прав субъектов персональных данных о предоставлении информации, необходимой для осуществления деятельности указанного органа, Оператор обязан сообщить такую информацию в уполномоченный орган в течение 30 дней с даты получения такого запроса.

2.13.5. В случае выявления неправомерной обработки персональных данных при обращении или по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

2.13.6. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором, последний в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных

данных. Об устранении допущенных нарушений Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.13.7. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных.

2.13.8. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

2.14. Режим конфиденциальности персональных данных.

2.14.1. Оператор обеспечивает конфиденциальность и безопасность персональных данных при их обработке в соответствии с требованиями законодательства РФ.

2.14.2. Оператор не раскрывает третьим лицам и не распространяет персональные данные без согласия на это субъекта персональных данных, если иное не предусмотрено Федеральным законом.

2.14.3. В соответствии с перечнем персональных данных, обрабатываемых в МИС IDENT, 1С: Фреш, СБИС персональные данные работника/клиента(пациента)/контрагента являются конфиденциальной информацией.

3. Обработка персональных данных

3.1. Получение персональных данных.

3.1.1. Все персональные данные следует получать от самого работника/клиента(пациента)/контрагента. В случае получения согласия на обработку персональных данных от представителя клиента(пациента)/контрагента полномочия данного представителя на дачу согласия от клиента/контрагента проверяются Оператором.

3.2. Лица, имеющие право доступа к персональным данным.

3.2.1. Правом доступа к персональным данным субъектов обладают лица, наделенные соответствующими полномочиями в соответствии со своими служебными обязанностями.

3.2.2. Перечень лиц, имеющих доступ к персональным данным, утверждается директором Оператора.

3.3. Порядок и сроки хранения персональных данных на МИС IDENT, 1С: Фреш, СБИС.

3.3.1. Оператор осуществляет хранение персональных данных работника/клиента(пациента)/контрагента на МИС IDENT, 1С: Фреш, СБИС.

3.3.2. Сроки хранения персональных данных: с момента предоставления данных работника/клиента(пациента)/контрагента до тех пор, пока работник/клиента(пациента)/контрагента не заявит о своем желании удалить свои персональные данные с МИС IDENT, 1С: Фреш, СБИС.

3.3.3. Оператором ведется обработка персональных данных на бумажных носителях информации.

3.3.4. Сроки хранения персональных данных на бумажных носителях информации в архиве Оператора 25 лет.

3.4. Блокирование персональных данных.

3.4.1. Под блокированием персональных данных понимается временное прекращение Оператором операций по их обработке по требованию работника/клиента(пациента)/контрагента при выявлении им недостоверности обрабатываемых сведений или неправомерных, по мнению субъекта персональных данных, действий в отношении его данных.

3.4.2. Оператор не передает персональные данные третьим лицам и не поручает обработку персональных данных сторонним лицам и организациям. Персональные данные клиента/контрагента обрабатывают только сотрудники Оператора (администраторы баз данных и т. д.), допущенные (приказом) к обработке персональных данных клиентов/контрагентов.

3.4.3. Блокирование персональных данных в МИС IDENT, 1С: Фреш, СБИС осуществляется на основании письменного заявления от субъекта персональных данных.

3.5. Уничтожение персональных данных.

3.5.1. Под уничтожением персональных данных понимаются действия, в результате которых становится невозможным восстановить содержание персональных данных на МИС IDENT, 1С: Фреш, СБИС и/или в результате которых уничтожаются материальные носители персональных данных.

3.5.2. Субъект персональных данных вправе в письменной форме требовать уничтожения своих персональных данных в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

3.5.3. В случае отсутствия возможности уничтожения персональных данных Оператор осуществляет блокирование таких персональных данных.

3.5.4. Уничтожение персональных данных осуществляется путем стирания информации с использованием сертифицированного программного обеспечения с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

4. Система защиты персональных данных

4.1. Меры по обеспечению безопасности персональных данных при их обработке.

4.1.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

4.1.2. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 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;
- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 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;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- назначением лица, ответственного за обработку персональных данных;
- установлением индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их должностными обязанностями;
- использованием сертифицированного антивирусного программного обеспечения;
- обучением работников Оператора, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных.

4.2. Защищаемые сведения о субъекте персональных данных.

К защищаемым сведениям о субъекте персональных данных на МИС IDENT, 1С: Фреш, СБИС относятся данные, позволяющие идентифицировать субъект персональных данных и/или получить о нем дополнительные сведения, предусмотренные законодательством и Положением.

4.3. Защищаемые объекты персональных данных.

4.3.1. К защищаемым объектам персональных данных в МИС IDENT, 1С: Фреш, СБИС относятся:

- объекты информатизации и технические средства автоматизированной обработки информации, содержащей персональные данные;
- информационные ресурсы (базы данных, файлы и др.), содержащие информацию об информационно-телекоммуникационных системах, в которых циркулируют персональные данные, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- каналы связи, которые используются для передачи персональных данных в виде информативных электрических сигналов и физических полей;
- отчуждаемые носители информации на магнитной, магнитно-оптической и иной основе, применяемые для обработки персональных данных.

4.3.2. Технологическая информация об информационных системах и элементах системы защиты персональных данных, подлежащая защите, включает:

- сведения о системе управления доступом на объекты информатизации, на которых осуществляется обработка персональных данных;
- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- характеристики каналов связи, которые используются для передачи персональных данных в виде информативных электрических сигналов и физических полей;
- информация о средствах защиты персональных данных, их составе и структуре, принципах и технических решениях защиты;

служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки персональных данных.

4.4. Требования к системе защиты персональных данных.

Система защиты персональных данных должна соответствовать требованиям постановления Правительства РФ от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.4.1. Система защиты персональных данных должна обеспечивать:

своевременное обнаружение и предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищенности персональных данных.

4.5. Ответственность.

4.5.1. Все сотрудники Оператора, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Положением, требованиями законодательства РФ.

4.5.2. Лица, виновные в нарушении требований Положения, несут предусмотренную законодательством РФ ответственность.

4.5.3. Ответственность за соблюдение режима персональных данных по отношению к персональным данным, находящимся в базах данных МИС IDENT, 1С: Фреш, СБИС, несут ответственные за обработку персональных данных.

5. Заключительные положения

5.1. В случае изменения действующего законодательства РФ, внесения изменений в нормативные документы по защите персональных данных настоящее Положение действует в части, не противоречащей действующему законодательству до приведения его в соответствие с такими.

5.2. Условия настоящего Положения устанавливаются, изменяются и отменяются Оператором в одностороннем порядке без предварительного уведомления работника/клиента(пациента)/контрагента. С момента размещения МИС IDENT, 1С: Фреш, СБИС новой редакции Положения предыдущая редакция считается утратившей свою силу.

5.3. Если работник/клиент(пациент)/контрагент не согласен с условиями настоящего Положения, то он должен немедленно сообщить Оператору об желании удалить свою карту с МИС IDENT, 1С: Фреш, СБИС, в противном случае продолжение использования работником/клиентом(пациентом)/контрагентом МИС IDENT, 1С: Фреш, СБИС означает, что работник/клиент(пациент)/контрагент согласен с условиями настоящего Положения.



В этом положении пронумеровано и
прошнуровано 10 листов.

М.П. (штамп)

Руководитель организации

Главный бухгалтер

Директор
Адолжность

«1» июня 2023 г.

подпись

Магаян А.О.

расшифровка подписи

Сечкарёва Н.А.

расшифровка подписи