УТВЕРЖДАЮ:
Генеральный директор
ООО «Стомион»
_____Политов А.С.
Приложение № 1 к приказу №9 от 30 декабря 2021 г.

ПОЛОЖЕНИЕ
о защите персональных данных пациентов в ООО «Стомион»

1. Термины и определения

1.1. **Персональные данные** — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, адрес электронной почты, телефонный номер, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.2. **Обработка персональных данных** — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование.

1.3. **Конфиденциальность персональных данных** — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.

1.4. **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.

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

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

1.7. **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.

1.8. **Обезличивание персональных данных** — действия, в результате которых невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.

1.9. **Общедоступные персональные данные** — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

1.11. **Субъект персональных данных** - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

1.12. **Оператор** - юридическое лицо, 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. В рамках настоящего Положения Оператором признается Общество с ограниченной ответственностью «Стомион» (далее Организация);

1.13 **Пациент** – физическое лицо (субъект), обратившееся в Организацию с целью получения платных медицинских стоматологических услуг;

1.14 **Законный представитель пациента** – лицо (родитель, усыновитель, опекун, попечитель), которое в силу закона (без особого полномочия) выступает во всех учреждениях в защиту прав и законных интересов недееспособных, ограниченно дееспособных и дееспособных пациентов, находящихся под попечительством;

1.15 **Работник** – физическое лицо, вступившее в трудовые отношения с Организацией;

1.16 **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью персональных компьютеров и ноутбуков;

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

1.18 **Медицинская информационная система** – комплексное программное обеспечение для персональных компьютеров и ноутбуков, используемое для автоматизации всех основных процессов, связанных с работой медицинского учреждения.

2. Общие положения

2.1. Настоящее Положение об обработке персональных данных (далее — Положение) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными федеральными законами.

2.2. Под обработкой и защитой персональных данных пациентов подразумевается в том числе обработка и защита персональных данных их законных представителей.

2.3. Цель разработки Положения — определение порядка обработки и защиты персональных данных всех пациентов Организации, данные которых подлежат обработке, на основании полномочий оператора; обеспечение 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, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.4. Порядок ввода в действие и изменения Положения.

2.4.1. Настоящее Положение вступает в силу с момента его утверждения генеральным директором Организации и действует бессрочно, до замены его новым Положением.

2.4.2. При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании Приказа генерального директора Организации

3. Состав персональных данных

3.1. В состав персональных данных пациентов в том числе входят:

3.1.1. Фамилия, имя, отчество.

3.1.2. Дата рождения.

3.1.3. Место рождения.

3.1.4. Адрес прописки (жительства, пребывания).

3.1.5. Семейное положение.

3.1.6. ИНН.

3.1.7. Паспортные данные.

3.1.8. Реквизиты полиса ДМС

3.1.9. Адрес электронной почты.

3.1.10. Номер телефона (домашний, сотовый).

3.1.11. Данные о состоянии здоровья (история болезни);

3.1.12. Биометрические данные пациента

3.1.13. Другая информация, необходимая для правильного проведения и медицинских исследований;

3.1.14. Результаты выполненных медицинских исследований.

3.2. В состав персональных данных законного представителя пациента в том числе входят:

3.2.1. Фамилия, имя, отчество.

3.2.2. Дата рождения.

3.2.3. Место рождения.

3.2.4. Адрес прописки (жительства, пребывания).

3.2.5. Семейное положение.

3.2.6. ИНН.

3.2.7. Паспортные данные.

3.2.8. Адрес электронной почты.

3.2.9. Номер телефона (домашний, сотовый).

4. Цель обработки персональных данных

4.1. Цель обработки персональных данных - осуществление комплекса действий направленных на достижение цели, в том числе:

4.1.1. Оказание консультационных и информационных услуг.

4.1.2. Оказание медицинских услуг, установления медицинского диагноза.

4.1.3. Иные сделки, не запрещенные законодательством, а также комплекс действий с персональными данными, необходимых для исполнения вышеуказанных сделок.

4.1.4. В целях исполнения требований законодательства РФ.

4.2. Условием прекращения обработки персональных данных является ликвидация Организации, а также соответствующее требование пациента.

5. Сбор, обработка и защита персональных данных

5.1. Порядок получения (сбора) персональных данных:

5.1.1. Все персональные данные пациента следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 5.1.4 и 5.1.6 настоящего Положения и иных случаях, предусмотренных законами РФ.

5.1.2. Согласие пациента на использование его персональных данных хранится в Организации в бумажном и/или электронном виде.

5.1.3. Согласие субъекта на обработку персональных данных действует в течение всего срока действия договора на оказание медицинских услуг. По истечении срока

действия договора на оказание медицинских услуг срок действия согласия на обработку персональных данных соответствует сроку хранения первичных медицинских документов и составляет 25 лет.

5.1.4. Если персональные данные пациента возможно получить только у третьей стороны, пациент (законный представитель пациента) должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Третье лицо, предоставляющее персональные данные пациента, должно обладать согласием субъекта на передачу персональных данных Организации. Организация обязана получить подтверждение от третьего лица, передающего персональные данные пациента о том, что персональные данные передаются с его согласия (согласия его законного представителя). Организация обязана при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся персональных данных пациентов.

5.1.5. Организация обязана сообщить пациенту (законному представителю пациента) о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента (законного представителя пациента) дать письменное согласие на их получение.

5.1.6. Обработка персональных данных пациентов без их согласия осуществляется в следующих случаях:

5.1.6.1. Персональные данные являются общедоступными.

5.1.6.2. По требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

5.1.6.3. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.

5.1.6.4. Обработка персональных данных осуществляется в целях заключения и исполнения договора, одной из сторон которого является субъект персональных данных – пациент.

5.1.6.5. Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.

5.1.6.6. В иных случаях, предусмотренных законом.

5.1.7. Организация не имеет права получать и обрабатывать персональные данные пациента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

5.2. Порядок обработки персональных данных:

5.2.1. Субъект персональных данных предоставляет Организации достоверные сведения о себе.

5.2.2. К обработке персональных данных пациентов могут иметь доступ только сотрудники Организации, допущенные к работе с персональными данными пациентов и подписавшие Соглашение о неразглашении коммерческой тайны. В список сведений, составляющих коммерческую тайну Организации, в том числе включены персональные данные пациента; сведения о порядке и состоянии организации охраны, системе сигнализации; данные об информационной системе персональных данных Организации и о применяемых способах информационной защиты; пароли пользователей к медицинской информационной системе Организации.

5.2.3. Право доступа к персональным данным пациентов в Организации имеют работники Организации: генеральный директор, главный врач, заместители главного врача, главный бухгалтер; заведующие всех подразделений; врачи; средний медицинский персонал (ассистенты врачей); младший медицинский персонал (медсестры); административный персонал (исполнительный директор, координатор по лечению, старшая медсестра, старший администратор, работники регистратуры); системный администратор, обеспечивающий работоспособность аппаратно-программных средств, предназначенных для автоматизированной обработки персональных данных; юрист; работники отдела кадров;

работники бухгалтерии; иные лица в силу своих должностных обязанностей.

5.2.4. Обработка персональных данных пациента может осуществляться исключительно в целях установленных Положением и соблюдения законов и иных нормативных правовых актов РФ.

5.2.5. Персональные данные пациентов хранятся на бумажных носителях и в электронном виде

5.2.6. Обработка персональных данных пациентов осуществляется смешанным путем: неавтоматизированным способом обработки персональных данных и автоматизированным способом обработки персональных данных (с помощью средств вычислительной техники и специальных программных продуктов).

5.2.7. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

5.2.8. При определении объема и содержания, обрабатываемых персональных данных Организация руководствоваться Конституцией Российской Федерации, законом о персональных данных и иными федеральными законами.

5.2.9. Контроль за хранением и использованием материальных носителей, содержащих персональные данные, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляет ответственное должностное лицо, осуществляющее обработку персональных данных.

5.3. Защита персональных данных:

5.3.1. Под защитой персональных данных пациента понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

5.3.2. Защита персональных данных пациента осуществляется за счёт Организации в порядке, установленном федеральным законом РФ.

5.3.3. Общую организацию защиты персональных данных пациента осуществляет генеральный директор Организации.

5.3.4. Доступ к персональным данным пациента имеют сотрудники Организации, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.

5.3.5. Все сотрудники, связанные с получением, обработкой и защитой персональных данных пациента, обязаны подписать Соглашение о неразглашении коммерческой тайны.

5.3.6. Процедура оформления доступа к персональным данным пациента включает в себя:

- Ознакомление сотрудника с настоящим Положением под роспись. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных пациента, с данными актами также производится ознакомление.

- Истребование с сотрудника (за исключением генерального директора) письменного обязательства о соблюдении конфиденциальности персональных данных пациента и соблюдении правил их обработки в соответствии с внутренними локальными актами Организации, регулирующих вопросы обеспечения безопасности конфиденциальной информации.

5.3.7. Сотрудник Организации, имеющий доступ к персональным данным пациента в связи с исполнением трудовых обязанностей:

- Обеспечивает хранение информации, содержащей персональные данные пациента, исключающее доступ к ним третьих лиц.

- В отсутствие сотрудника на его рабочем месте не должно быть документов,

содержащих персональные данные пациентов.

- При уходе в отпуск, во время служебной командировки и в иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные пациентов лицу, на которое локальным актом Общества (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные пациентов, передаются другому сотруднику, имеющему доступ к персональным данным пациентов по указанию генерального директора Организации.

- При увольнении сотрудника, имеющего доступ к персональным данным пациентов, документы и иные носители, содержащие персональные данные пациентов, передаются другому сотруднику, имеющему доступ к персональным данным пациентов по указанию генерального директора.

- В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией генерального директора, доступ к персональным данным пациентов может быть предоставлен иному сотруднику. Допуск к персональным данным пациентов других сотрудников Организации, не имеющих надлежащим образом оформленного доступа, запрещается.

5.4. Хранение персональных данных:

5.4.1. Документы на бумажных носителях, содержащие персональные данные пациентов хранятся в специально отведенном для хранения персональных данных помещении, обеспечивающем сохранность персональных данных пациентов и защищенном от несанкционированного доступа.

5.4.2. Персональные данные пациентов в электронном виде хранятся в локальной компьютерной сети Организации, в используемой в Организации медицинской информационной системе, в электронных папках и файлах в персональных компьютерах и ноутбуках генерального директора и сотрудников, допущенных к обработке персональных данных пациентов.

5.4.3. Защита доступа к электронным базам данных, содержащим персональные данные пациентов, обеспечивается:

- Использованием лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный вход в локальную сеть Организации.

- Разграничением прав доступа к используемой в Организации медицинской информационной системы с использованием учетной записи.

- Двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли к учетным записям медицинской информационной системы устанавливаются генеральным директором Организации и сообщаются индивидуально сотрудникам, имеющим доступ к персональным данным пациентов.

5.4.3.1. Несанкционированный вход в ПК или ноутбук, в которых содержатся персональные данные пациентов, блокируется паролем, который устанавливается ответственным за персональный компьютер или ноутбук сотрудником, и не подлежит разглашению.

5.4.3.2. Все электронные папки и файлы, содержащие персональные данные пациентов, защищаются паролем, который устанавливается генеральным директором организации.

5.4.3.3. Изменение паролей генеральным директором осуществляется не реже 1 раза в 3 месяца.

5.4.4. Копировать и делать выписки персональных данных пациента разрешается исключительно в служебных целях с письменного разрешения генерального директора Организации.

5.4.5. Ответы на письменные запросы других организаций и учреждений о персональных данных пациентов даются только с письменного согласия самого пациента, если иное не установлено законодательством. Ответы оформляются в письменном виде, на

бланке Организации, и в том объеме, который позволяет не разглашать излишний объем персональных данных пациента.

6. Передача персональных данных

6.1. Передача персональных данных:

6.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

6.1.2. При передаче персональных данных работники Организации должны соблюдать следующие требования:

6.1.2.1. Не сообщать персональные данные пациента в коммерческих целях.

6.1.2.2. Не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, установленных федеральным законом РФ.

6.1.2.3. Предупредить лиц, получающих персональные данные пациента о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

6.1.2.4. Разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные пациентов, которые необходимы для выполнения конкретных функций.

6.1.2.5. Осуществлять передачу персональных данных пациента в пределах Организации в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.

6.1.2.6. Предоставлять доступ пациента к своим персональным данным при обращении либо при получении запроса пациента. Организация обязана сообщить пациенту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение десяти рабочих дней с момента обращения.

6.1.2.7. Передавать персональные данные пациента представителям пациента в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

6.1.2.8. Обеспечивать ведение журнала учета выданных персональных данных пациентов, в котором фиксируются сведения о лице, которому передавались персональные данные пациентов, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана.

7. Сроки и порядок обработки и хранения персональных данных

7.1. Обработка персональных данных пациентов осуществляется в течение всего периода лечения.

7.2. Хранение документов, содержащих персональные данные пациентов, осуществляется в течение сроков, установленных законодательными нормативными актами Российской Федерации в отношении данных документов.

7.3. Срок хранения персональных данных, внесенных в информационную систему персональных данных, должен соответствовать сроку хранения бумажных носителей персональных данных.

7.4. Сроки хранения персональных данных:

7.4.1. Сроки хранения гражданско-правовых договоров на оказание медицинских услуг, содержащих персональные данные пациентов, а также сопутствующих их заключению, исполнению документов – 5 лет с момента окончания действия договоров.

7.4.2. Срок хранения медицинской карты стоматологического пациента – 25 лет.

7.4.3. Срок хранения медицинской карты ортодонтического пациента – 25 лет.

7.5. В течение срока хранения персональные данные не могут быть обезличены или уничтожены.

7.6. По истечении установленных сроков хранения документы, содержащие персональные данные пациентов, подлежат уничтожению.

7.7. Персональные данные пациентов, содержащихся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных.

8. Права пациента

Пациент имеет право:

8.1. Ознакомиться с настоящим Положением.

8.2. Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

8.3. Требовать перечень обрабатываемых персональных данных, имеющихся в Организации и источник их получения.

8.4. Получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения.

8.5. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.6. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

8.7. Отозвать свое согласие на обработку персональных данных посредством составления соответствующего письменного документа, который может быть направлен Организации заказными письмом с уведомлением либо вручен лично работнику регистратуры Организации.

9. Права оператора персональных данных

Организация вправе:

9.1. Отстаивать свои интересы в суде.

9.2. Предоставлять персональные данные пациентов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

9.3. Отказать в предоставлении персональных данных в случаях, предусмотренных законом.

9.4. Использовать персональные данные пациента без его согласия, в случаях предусмотренных законодательством РФ.

9.5. Продолжить обработку данных о здоровье пациента в медико-профилактических целях согласно п.2 ст.9 № 152-ФЗ даже в случае отзыва пациентом согласия на обработку персональных данных.

10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

10.1. Работники Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующем законодательством Российской Федерации и внутренними олкальными актами Организации.