общество с ограниченной ответственностью

«Стоматологическая клиника Владимира Новикова»

ООО «СКВН», ИНН 7704236252, КПП 770401001

УТВЕРЖДЕНО
28.09.2017 года

ПОЛОЖЕНИЕ
о защите персональных данных Пациентов (Заказчиков) в ООО «Стоматологическая клиника Владимира Новикова»

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. Пациент (Заказчик) (субъект персональных данных) - физическое лицо, потребитель услуг ООО «СКВН», далее «Организация».
1.12. 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. В рамках настоящего Положения Оператором признается Общество с ограниченной ответственностью «СКВН»;

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 "Об информации, информационных технологиях и о защите информации", Федеральным законом 152-ФЗ "О персональных данных", иными федеральными законами.
2.2. Цель разработки Положения — определение порядка обработки и защиты персональных данных всех

Клиентов 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.

2.3. Порядок ввода в действие и изменения Положения.

2.3.1. Настоящее Положение вступает в силу с момента его утверждения Заместителем генерального директора Организации и действует бессрочно, до замены его новым Положением.

2.3.2. Изменения в Положение вносятся на основании Приказов Заместителя генерального директора Организации.

3. Состав персональных данных.

3.1. В состав персональных данных Пациентов (Заказчиков), в том числе входят:

3.1.1. Фамилия, имя, отчество.

3.1.2. Год рождения.

3.1.3. Месяц рождения.

3.1.4. Дата рождения.

3.1.5. Место рождения.

3.1.7. Семейное положение.

3.1.8. Образование.

3.1.9. Профессия.

3.1.10. Доходы.

3.1.11. ИНН, номер Пенсионного свидетельства.

3.1.12. Место работы.

3.1.13. Занимаемая должность.

3.1.14. Адрес электронной почты.

3.1.15. Номер телефона (домашний, сотовый).

3.2. В Организации могут создаваться (создаются, собираются) и хранятся следующие документы и сведения, в том числе в электронном виде, содержащие данные о Пациентах (Заказчиках):

3.2.1. Анкета.

3.2.2. Заявка на регистрацию — физического лица.

3.2.3. Договор (публичная оферта).

3.2.4. Подтверждение о присоединении к договору.

3.2.5. Копии документов, удостоверяющих личность, а также иных документов, предоставляемых Пациентом (Заказчиком), и содержащих персональные данные.

3.2.6. Данные по оплатам заказов (товаров/услуг), содержащие платежные и иные реквизиты Пациента (Заказчика).

3.2.7. Записи телефонных переговоров и электронная переписка.

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

4.1.3. В целях исполнения требований законодательства РФ.

4.2. Условием прекращения обработки персональных данных является ликвидация Организации, а также соответствующее требование Пациентов (Заказчиков).

5. Сбор, обработка и защита персональных данных.

5.1. Порядок получения (сбора) персональных данных:

5.1.1. Все персональные данные Пациентов (Заказчиков) 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 Пациентов (Заказчиков) 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, а также в течение 5 лет с даты прекращения действия договорных отношений Пациентов (Заказчиков) с Организацией. По истечении указанного срока действие согласия считается продленным на каждые следующие пять лет при отсутствии сведений о его отзыве.
5.1.4. Если персональные данные Пациента (Заказчика) возможно получить только у третьей стороны, Пациент (Заказчик) должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Третье лицо, предоставляющее персональные данные Пациента (Заказчика), должно обладать согласием субъекта на передачу персональных данных Организации. Организация обязана получить подтверждение от третьего лица, передающего персональные данные Пациента (Заказчика) о том, что персональные данные передаются с его согласия. Организация обязана при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся персональных данных Пациентов (Заказчиков).

5.1.5. Организация обязана сообщить Пациенту (Заказчику) о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Пациента (Заказчика) персональных данных дать письменное согласие на их получение.
5.1.6. Обработка персональных данных Пациентов (Заказчиков) 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 (Заказчик).
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 (Заказчика) о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, 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 (Заказчиков) могут иметь доступ только сотрудники Организации, допущенные к работе с персональными данными Пациента (Заказчика) и подписавшие Соглашение о неразглашении персональных данных Пациента (Заказчика).
5.2.3. Право доступа к персональным данным Пациента (Заказчика) в Организации имеют:
• Генеральный директор Организации;
• Работники, ответственные за ведение операционной работы (Финансовый отдел).
• Работники Отдела по работе с Клиентами (CRM).
• Работники службы безопасности.
• Работники службы внутреннего контроля.
• Работники юридической службы. • Работники IT (Отдел информационных технологий).
• Работники службы документационного обеспечения (Группа по документообороту).
• Клиент, как субъект персональных данных.
5.2.3.1. Поименный перечень сотрудников Организации, имеющих доступ к персональным данным Пациентов (Заказчиков), определяется приказом Заместителя генерального директора Организации.
5.2.4. Обработка персональных данных Пациента (Заказчика) может осуществляться исключительно в целях установленных Положением и соблюдения законов и иных нормативных правовых актов РФ.
5.2.5. При определении объема и содержания, обрабатываемых персональных данных Организация руководствоваться Конституцией Российской Федерации, законом о персональных данных, и иными федеральными законами.
5.3. Защита персональных данных:
5.3.1. Под защитой персональных данных Пациента (Заказчика) 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 (Заказчика) осуществляется за счёт Организации в порядке, установленном федеральным законом РФ.

5.3.3. Организация при защите персональных данных Пациентов (Заказчиков) принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:
• Шифровальные (криптографические) средства.
• Антивирусная защита.
• Анализ защищённости.
• Обнаружение и предотвращение вторжений.
• Управления доступом.
• Регистрация и учет.
• Обеспечение целостности.
• Организация нормативно-методических локальных актов, регулирующих защиту персональных данных.
5.3.4. Общую организацию защиты персональных данных Пациентов (Заказчиков) осуществляет Заместитель генерального директора Организации.
5.3.5. Доступ к персональным данным Пациента (Заказчика) имеют сотрудники Организации, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.
5.3.6. Все сотрудники, связанные с получением, обработкой и защитой персональных данных Пациентов (Заказчиков), обязаны подписать Соглашение о неразглашении персональных данных Пациентов (Заказчиков).
5.3.7. Процедура оформления доступа к персональным данным Пациента (Заказчика) включает в себя:
• Ознакомление сотрудника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных Пациента (Заказчика), с данными актами также производится ознакомление под роспись.
• Истребование с сотрудника (за исключением Генерального директора) письменного обязательства о соблюдении конфиденциальности персональных данных Пациентов (Заказчиков) и соблюдении правил их обработки в соответствии с внутренними локальными актами Организации, регулирующих вопросы обеспечения безопасности конфиденциальной информации.
5.3.8. Сотрудник Организации, имеющий доступ к персональным данным Пациентов (Заказчиков) в связи с исполнением трудовых обязанностей:
• Обеспечивает хранение информации, содержащей персональные данные Пациента (Заказчика), исключающее доступ к ним третьих лиц.
• В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные Пациентов (Заказчиков).
• 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 (Заказчиков) 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 (Заказчиков), передаются другому сотруднику, имеющему доступ к персональным данным Пациентов (Заказчиков) по указанию Заместителя генерального директора Организации.
• При увольнении сотрудника, имеющего доступ к персональным данным Пациентов (Заказчиков), документы и иные носители, содержащие персональные данные Пациентов (Заказчиков), передаются другому сотруднику, имеющему доступ к персональным данным Пациентов (Заказчиков) по указанию Генерального директора.
• В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией Заместителя Генерального директора, доступ к персональным данным Пациента (Заказчика) может быть предоставлен иному сотруднику. Допуск к персональным данным Пациента (Заказчика) других сотрудников Организации, не имеющих надлежащим образом оформленного доступа, запрещается.
5.3.9. Менеджер по кадровой работе обеспечивает:
• Ознакомление сотрудников под роспись с настоящим Положением.
• Истребование с сотрудников письменного обязательства о соблюдении конфиденциальности персональных данных Пациента (Заказчика) (Соглашение о неразглашении) и соблюдении правил их обработки.
• Общий контроль за соблюдением сотрудниками мер по защите персональных данных Пациента (Заказчика).
5.3.10. Защита персональных данных Пациентов (Заказчиков), хранящихся в электронных базах данных Организации, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается Системным администратором.
5.4. Хранение персональных данных:

5.4.1. Персональные данные Пациентов (Заказчиков) на бумажных носителях хранятся в специально отведенном месте.
5.4.2. Персональные данные Пациентов (Заказчиков) в электронном виде хранятся в локальной компьютерной сети Организации, в электронных папках и файлах в персональных компьютерах Заместителя генерального директора и сотрудников, допущенных к обработке персональных данных Пациентов (Заказчиков).
5.4.3. Документы, содержащие персональные данные Пациентов (Заказчиков), хранятся в запирающихся шкафах, обеспечивающих защиту от несанкционированного доступа. В конце рабочего дня все документы, содержащие персональные данные Пациентов (Заказчиков), помещаются в шкафы, обеспечивающие защиту от несанкционированного доступа.
5.4.4. Защита доступа к электронным базам данных, содержащим персональные данные Пациентов (Заказчиков), обеспечивается:
• Использованием лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный вход в локальную сеть Организации.
• Разграничением прав доступа с использованием учетной записи.
• Двух ступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются Системным администратором Организации и сообщаются индивидуально сотрудникам, имеющим доступ к персональным данным Пациентов (Заказчиков).
5.4.4.1. Несанкционированный вход в ПК, в которых содержатся персональные данные Пациентов (Заказчиков), блокируется паролем, который устанавливается Системным администратором и не подлежит разглашению.
5.4.4.2. Все электронные папки и файлы, содержащие персональные данные Пациентов (Заказчиков), защищаются паролем, который устанавливается ответственным за ПК сотрудником Организации и сообщается Системному администратору.
5.4.4.3. Изменение паролей Системным администратором осуществляется не реже 1 раза в 6 месяцев.
5.4.5. Копировать и делать выписки персональных данных Пациента (Заказчика) разрешается исключительно в служебных целях с письменного разрешения Генерального директора Организации.
5.4.6. Ответы на письменные запросы других организаций и учреждений о персональных данных Пациентов (Заказчиков) даются только с письменного согласия самого Пациента (Заказчика), 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 (Заказчика).

6. Блокировка, обезличивание, уничтожение персональных данных

6.1. Порядок блокировки и разблокировки персональных данных:
6.1.1. Блокировка персональных данных Пациентов (Заказчиков) осуществляется с письменного заявления Пациентов (Заказчиков).
6.1.2. Блокировка персональных данных подразумевает:
6.1.2.1. Запрет редактирования персональных данных.
6.1.2.2. Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).
6.1.2.3. Запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).
6.1.2.4. Изъятие бумажных документов, относящихся к Пациенту (Заказчику) и содержащих его персональные данные из внутреннего документооборота Организации и запрет их использования.
6.1.3. Блокировка персональных данных Пациента (Заказчика) может быть временно снята, если это требуется для соблюдения законодательства РФ.
6.1.4. Разблокировка персональных данных Пациента (Заказчика) осуществляется с его письменного согласия (при наличии необходимости получения согласия) или заявления Пациента (Заказчика).
6.1.5. Повторное согласие Пациента (Заказчика) на обработку его персональных данных (при необходимости его получения) влечет разблокирование его персональных данных.
6.2. Порядок обезличивания и уничтожения персональных данных:
6.2.1. Обезличивание персональных данных Пациента (Заказчика) происходит по письменному заявлению Клиента, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.
6.2.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному Пациенту (Заказчику).
6.2.3. Бумажные носители документов при обезличивании персональных данных уничтожаются.
6.2.4. Организация обязана обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести

обезличивание персональных данных в передаваемых разработчику информационных системах.
6.2.5. Уничтожение персональных данных Пациента (Заказчика) подразумевает прекращение какого-либо доступа к персональным данным Пациента (Заказчика).
6.2.6. При уничтожении персональных данных Пациента (Заказчика) работники Организации не могут получить доступ к персональным данным субъекта в информационных системах.
6.2.7. Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.
6.2.8. Операция уничтожения персональных данных необратима.
6.2.9. Срок, после которого возможна операция уничтожения персональных данных Пациента (Заказчика), определяется окончанием срока, указанным в пункте 7.3 настоящего Положения.

7. Передача и хранение персональных данных

7.1. Передача персональных данных:
7.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.
7.1.2. При передаче персональных данных работники Организации должны соблюдать следующие требования:
7.1.2.1. Не сообщать персональные данные Пациента (Заказчика) в коммерческих целях.
7.1.2.2. Не сообщать персональные данные Пациента (Заказчика) третьей стороне без письменного согласия Пациента (Заказчика), за исключением случаев, установленных федеральным законом РФ.
7.1.2.3. Предупредить лиц, получающих персональные данные Пациента (Заказчика) 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;
7.1.2.4. Разрешать доступ к персональным данным Пациентов (Заказчиков) только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Пациентов (Заказчиков), которые необходимы для выполнения конкретных функций.
7.1.2.5. Осуществлять передачу персональных данных Пациента (Заказчика) в пределах Организации в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.
7.1.2.6. Предоставлять доступ Пациента (Заказчика) к своим персональным данным при обращении либо при получении запроса Пациента (Заказчика). Организация обязана сообщить Пациенту (Заказчику) информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение десяти рабочих дней с момента обращения.
7.1.2.7. Передавать персональные данные Пациента (Заказчика) его представителям 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.
7.1.2.8. Обеспечивать ведение журнала учета выданных персональных данных Пациентов (Заказчиков), в котором фиксируются сведения о лице, которому передавались персональные данные Пациентов (Заказчиков), дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана (по форме Приложения №1).
7.2. Хранение и использование персональных данных:
7.2.1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.
7.2.2. Персональные данные Пациентов (Заказчиков) обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Организации. Персональные данные Пациентов (Заказчиков) также хранятся в электронном виде: в локальной компьютерной сети Организации, в электронных папках и файлах в ПК Генерального директора и работников, допущенных к обработке персональных данных Пациентов (Заказчиков).
7.2.3. Хранение персональных данных Пациента (Заказчика) может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами РФ.
7.3. Сроки хранения персональных данных:
7.3.1. Сроки хранения гражданско-правовых договоров, содержащих персональные данные Пациентов (Заказчиков), а также сопутствующих их заключению, исполнению документов - 5 лет с момента окончания действия договоров.
7.3.2. В течение срока хранения персональные данные не могут быть обезличены или уничтожены.
7.3.3. По истечении срока хранения персональные данные могут быть обезличены в информационных

системах и уничтожены на бумажном носителе в порядке установленном в Положении и действующем законодательстве РФ.

8. Права оператора персональных данных

Организация вправе:
8.1. Отстаивать свои интересы в суде.
8.2. Предоставлять персональные данные Пациентов (Заказчиков) третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).
8.3. Отказать в предоставлении персональных данных в случаях, предусмотренных законом.
8.4. Использовать персональные данные Пациента (Заказчика) без его согласия, в случаях предусмотренных законодательством РФ.

9. Права Пациента (Заказчика)

Пациент (Заказчик) имеет право:
9.1. 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;
9.2. Требовать перечень обрабатываемых персональных данных, имеющихся в Организации и источник их получения.
9.3. Получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения.
9.4. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.
9.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его 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 локальными актами Организации.