ПОЛИТИКА **в отношении обработки персональных данных**

1. Общие положения

1.1. Настоящая Политика в отношении персональных данных (далее - Политика) определяет порядок сбора, систематизации, накопления, уточнения, использования, хранения, распространения и защиты персональных данных работников и клиентов (потребителей услуг, пациентов) ООО «Стоматологическая клиника Перцева С.С.» (Далее – Клиника).

1.2. Настоящая Политика разработана в строгом соответствии с требованиями:

- Конституции РФ;
- Трудового кодекса РФ;
- Гражданского кодекса РФ;
- Перечня сведений конфиденциального характера, утв. Указом Президента от 06.03.1997 № 188;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 21.07.2014 № 242 «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;
- Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. В настоящей Политике используются следующие термины и понятия:

Работник - физическое лицо, состоящее в трудовых отношениях с работодателем.

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (сведения о фактах, обстоятельствах и событиях частной жизни).

Клиент (пациент) - физическое лицо, выступающее стороной в гражданско-правовом договоре на оказание медицинских услуг.

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.

Защита персональных данных - деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном работнике, клиенте.

Конфиденциальная информация - это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

2. Защита персональных данных работников

2.1. Состав персональных данных работника, обрабатываемых в Клинике

Персональные данные работников (лиц, являющихся стороной трудового договора), которые обрабатываются в Клинике:

- паспортные данные (Ф. И. О., дата рождения, место рождения, место регистрации, семейное положение, наличие или отсутствие детей);
- данные трудовой книжки работника (информация обо всех местах работы по трудовому договору, поощрениях);
- номер страхового свидетельства государственного пенсионного страхования;
- информация из документов воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- информация об образовании, о квалификации или наличии специальных знаний;
- информация о предварительных, периодических медицинских осмотрах;
- информация о прививках (вакцинопрофилактике);

- информация о факте беременности женщины;
- информация об инвалидности.

2.2. Обработка персональных данных работника

2.2.1. В целях обеспечения прав и свобод человека и гражданина работодатель при обработке персональных данных работника обязан соблюдать следующие общие требования:

- персональные данные работника могут обрабатываться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, обеспечения личной и имущественной безопасности работников;
- все персональные данные (Ф. И. О., дата и место рождения, адрес, семейное положение, образование, профессия работника, а также иная информация, необходимая в связи с трудовыми отношениями) следует получать лично у работника.

2.2.2. Если персональные данные работника можно получить только у третьей стороны, работник должен быть уведомлен об этом за 3 (три) дня и от него должно быть получено письменное согласие (либо отказ), которое работник должен дать в течение 5 (пяти) дней с даты получения уведомления.

2.2.3. Сведения о работниках организации хранятся на бумажных носителях в кабинете руководителя. Для этого используются специально оборудованный сейф. Ключ от сейфа находится у руководителя организации.

2.2.4. Конкретные обязанности по хранению личных дел работников, заполнению, хранению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, отражающих персональные данные работников, возлагаются на руководителя в соответствии с его должностными обязанностями, закрепленными в должностной инструкции.

2.2.5. Сведения о работниках организации могут также храниться на электронных носителях, доступ к которым ограничен паролем.

2.2.6. Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным законом либо работодателем на получение соответствующих сведений.

2.2.7. При получении сведений, составляющих персональные данные работников, указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, заданий.

2.2.8. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, 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;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые определяют возможность выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом и настоящей Политикой, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Перечисленные требования установлены Трудовым кодексом (ст. 88) и не подлежат изменению, так как являются обязательными для сторон трудовых отношений.

2.3. Обязанности работника и работодателя при обработке персональных данных

Обязанности работника

2.3.1. При поступлении на работу работник предоставляет свои персональные данные в форме документов:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка, за исключением случаев, когда работник поступает на работу впервые или на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;
- в отдельных случаях с учетом специфики работы действующим законодательством может предусматриваться предъявление иных документов.

2.3.2. В случае изменения сведений, составляющих персональные данные, работник должен незамедлительно предоставить данную информацию работодателю.

Обязанности работодателя

2.3.3. Работодатель обязан:

- обеспечить защиту персональных данных работника;
- обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, по учету использования рабочего времени и расчетов с работниками по оплате труда (персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные);
- заполнять документацию, содержащую персональные данные работника, преимущественно в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, если иные формы не утверждены в Клинике;
- выдавать работнику копии документов, связанных с работой, по письменному заявлению работника не позднее 3 (трех) дней со дня подачи заявления. Копии документов, связанных с работой (приказа о приеме на работу, приказов о переводе на другую работу, приказа об увольнении, выписки из трудовой книжки, справки о заработной плате и др.), должны заверяться надлежащим образом и предоставляться работнику лично.

2.3.4. Работодатель не имеет права:

- получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях, частной жизни;
- получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законом;
- при принятии решений, затрагивающих интересы работников, основываться на персональных данных работника, полученных в результате их автоматизированной обработки.

2.4. Права работников в целях защиты персональных данных

2.4.1. В целях защиты персональных данных, хранящихся у работодателя, работник вправе:

- получать полную информацию о его персональных данных и обработке этих данных, в частности, работник имеет право знать, кто и в каких целях использует или использовал его персональные данные;
- иметь свободный доступ к своим персональным данным, в том числе получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определять лиц для защиты своих персональных данных;
- требовать исключения или дополнения, а также исправления неверных или неполных персональных данных; дополнять данные оценочного характера заявлением, выражающим его собственную точку зрения;
- обжаловать в судебном порядке любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

3. Персональные данные клиентов (потребителей услуг, пациентов)

3.1. Состав сведений (персональных данных) о клиентах и цели их обработки

3.1.1. Персональные данные пациентов (лиц, являющихся стороной договора на оказание медицинских услуг), обрабатываемые в Клинике:

- паспортные данные;
- номера телефонов для связи с клиентом (контактная информация);
- информация о состоянии здоровья пациента, поставленных диагнозах, проведенном или планируемом к проведению медицинском вмешательстве, случаях обращения за медицинской помощью.

3.1.2. Персональные данные клиентов, полученные при заключении договора оказания медицинских услуг, обрабатываются только в целях предоставления услуг, качественной медицинской помощи, проведения оценки качества оказываемых услуг.

3.1.3. Клиника обеспечивает конфиденциальность персональных данных клиентов и обязана не допускать их распространения без согласия клиентов либо наличия иного законного основания.

3.1.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиентов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.2. Порядок обработки персональных данных клиентов

3.2.1. Клиника получает персональные данные непосредственно от субъекта персональных данных - клиента на основании заключения с клиентом письменного договора на оказание медицинских услуг.

3.2.2. Клиникой берется согласие на обработку персональных данных пациентов с целью демонстрации пациентам серьезности намерений соблюдения конфиденциальности, а также с целью предупреждения о тех случаях, когда информация о здоровье пациента может быть передана третьим лицам без его согласия.

3.2.3. Персональные данные клиента обрабатываются Клиникой исключительно для достижения целей,

определенных письменным договором между клиентом и Клиникой, в частности, для оказания медицинских услуг клиенту.

3.2.4. Обработка персональных данных клиентов ведется методом смешанной (в том числе автоматизированной) обработки.

3.2.5. К обработке персональных данных клиента могут иметь доступ только сотрудники Клиники, допущенные к работе с персональными данными клиента.

3.2.6. Отзыв пациентом согласия на обработку персональных данных о здоровье не влечет прекращения обработки персональных данных в силу части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ.

3.2.7. Клиника уничтожает персональные данные клиента, за исключением данных, содержащихся в медицинской карте и иной медицинской документации, в следующие сроки: в течение **7 (семи)** рабочих дней с момента расторжения договора или отзыва согласия на обработку при условии завершения расчетов между Клиникой и клиентом.

3.2.8. Без согласия клиента персональные данные о состоянии его здоровья могут быть переданы в случаях, прямо предусмотренных статьей 13 Федерального закона от 21.11.2011 № 323-ФЗ, **в случае возникновения угрозы распространения инфекционных заболеваний** (гепатиты, ВИЧ, сифилис, ОРИ, туберкулез), о чем клиент уведомляется в согласии на обработку его персональных данных.

3.2.9. Персональные данные клиентов содержатся в следующих документах:

- договор оказания медицинских услуг и все приложения к нему;
- анкета о здоровье;
- медицинская карта;
- информированные согласия на различные виды медицинских манипуляций.

3.2.10. Персональные данные клиентов могут храниться как на бумажных носителях, так и в электронном виде.

3.2.11. Персональные данные клиентов на бумажных носителях, если с них не снят на законном основании режим конфиденциальности, хранятся в специально отведенных шкафах. Ключи от шкафов хранятся у соответствующего специалиста, допущенного к обработке персональных данных клиентов.

3.2.12. Персональные данные клиентов также хранятся в электронном виде - в локальной компьютерной сети Клиники, в базах данных и файлах, размещенных на серверах Клиники, доступ к которым разрешен сотрудникам, допущенным к обработке персональных данных клиентов.

3.2.13. При передаче персональных данных клиента Клиника должна соблюдать следующие требования:

- не сообщать персональные данные клиента третьей стороне без письменного согласия клиента, за исключением случаев, установленных федеральным законом;
- не сообщать персональные данные клиента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные клиента 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;
- разрешать доступ к персональным данным клиентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные клиентов, которые необходимы для выполнения конкретных функций.

3.3. Права и обязанности Клинике при обработке персональных данных клиента

3.3.1. В целях обеспечения прав и свобод человека и гражданина Клиника и ее сотрудники при обработке персональных данных клиента обязаны соблюдать следующие общие требования:

- при определении объема и содержания персональных данных клиента, подлежащих обработке, руководствоваться федеральными законами от 27.07.2006 № 152-ФЗ и от 21.11.2011 № 323-ФЗ, а также договорными обязательствами, взятыми на себя сторонами по договору между клиентом и Клиникой;
- не получать и не обрабатывать персональные данные клиента о его судимости, политических, религиозных и иных убеждениях и частной жизни.

3.3.2. Клиника должна обеспечить защиту персональных данных клиента от неправомерного их использования или утраты за собственный счет в порядке, установленном федеральным законодательством.

3.3.3. Клиника обязана сообщить клиенту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомиться с ними.

3.3.4. Все сотрудники, связанные с получением, обработкой и защитой персональных данных клиентов, обязаны подписать уведомление-обязательство о неразглашении персональных данных клиентов.

Процедура оформления доступа к персональным данным клиента включает:

- ознакомление сотрудника под подпись с настоящей Политикой. При наличии иных нормативных актов (приказов, распоряжений, инструкций), регулирующих обработку и защиту персональных данных клиента, с данными актами также производится ознакомление под подпись;
- уведомление сотрудника о факте обработки персональных данных;

- истребование с сотрудника (за исключением директора) письменного обязательства о соблюдении конфиденциальности персональных данных клиентов и соблюдении правил их обработки.

3.3.5. Сотрудник Клинике, имеющий доступ к персональным данным клиентов в связи с исполнением трудовых обязанностей, **обязан**:

- обеспечивать хранение информации, содержащей персональные данные клиента, исключаящее доступ к ним третьих лиц;
- не оставлять на рабочем месте документы, содержащие персональные данные клиентов;
- при уходе в отпуск, во время болезни и в иных случаях длительного отсутствия передать документы и иные носители, содержащие персональные данные клиентов, директору Клинике.

3.4. Права и обязанности клиента

3.4.1. Клиент обязан передавать Клинике или ее представителю комплекс достоверных, документированных персональных данных, состав которых установлен настоящей Политикой и договорными обязательствами, взятыми на себя сторонами по договору между клиентом и Клиникой.

3.4.2. Клиент должен без неоправданной задержки сообщать Клинике об изменении своих персональных данных.

3.4.3. Клиент имеет право на получение сведений о Клинике, о ее местонахождении, о наличии у Клинике персональных данных, относящихся к клиенту, а также на ознакомление с такими персональными данными.

Клиент вправе требовать от Клинике 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.

3.4.4. Доступ клиента к своим персональным данным предоставляется на основании письменного запроса пациента на имя руководителя Клинике. Запрос должен содержать номер основного документа, удостоверяющего личность клиента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись клиента или его законного представителя.

3.4.5. Клиент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Клиникой, а также цель такой обработки;
- способы обработки персональных данных, применяемые Клиникой;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для клиента может повлечь обработка его персональных данных.

3.4.6. Клиент имеет право отозвать согласие на обработку персональных данных, ограничить способы и формы обработки персональных данных, запретить распространение персональных данных без его согласия. Отзыв пациентом согласия на обработку персональных данных о здоровье не влечет прекращения обработки персональных данных в силу части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ.

3.4.7. Клиент вправе обжаловать действия или бездействие Клинике в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

3.4.8. Клиент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

4. Система мер защиты персональных данных

4.1. Общую организацию защиты персональных данных клиентов осуществляет директор Клинике.

4.2. Защиту персональных данных, хранящихся в электронных базах данных Клинике, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий обеспечивает специалист, оказывающий услуги на основании договора подряда.

4.3. Система организационно-технических мер защиты персональных данных определяется в отдельных локально-нормативных актах Клинике в соответствии с действующими требованиями российского законодательства к защите персональных данных при их обработке в зависимости от типа угроз.

Помимо организационно-технических мер Клиника принимает правовые меры для защиты персональных данных, а именно издает локальные правовые акты, направленные на регулирование обработки персональных данных в рамках Клинике:

- Политика в отношении обработки персональных данных в организации;

- приказ о назначении ответственного за обработку персональных данных;
- приказ об утверждении перечня обрабатываемых персональных данных;
- приказ о допуске сотрудников к обработке персональных данных;
- приказ об обработке персональных данных без использования средств автоматизации;
- приказ о разработке комплекса организационно-технических мер по защите персональных данных с использованием средств автоматизации;
- приказ о форме запросов субъектов персональных данных и др.

5. Ответственность за разглашение персональных данных

5.1. Клиника несет ответственность за разработку, введение и действенность соответствующих требованиям законодательства норм, регламентирующих получение, обработку и защиту персональных данных клиента и сотрудников. Клиника закрепляет персональную ответственность сотрудников за соблюдение установленного в организации режима конфиденциальности.

5.2. Руководитель, разрешающий доступ сотрудника к документам, содержащим персональные данные клиента, несет персональную ответственность за данное разрешение.

5.3. Каждый сотрудник Клиники, получающий для работы документ, содержащий персональные данные клиента, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

5.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных клиента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами:

- Гражданского кодекса - гражданско-правовая ответственность (ст. ст. 150, 151);
- КоАП - административная ответственность (ст. ст. 13.14);
- Уголовного кодекса - уголовная ответственность (ст. 137).

5.5. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных клиентов Клиника вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания, в том числе увольнение на основании статьи 81 Трудового кодекса (подпункта «в» пункта б) за разглашение персональных данных другого работника.

6. Заключительные положения

Настоящее Положение вступает в силу с момента издания приказа директора организации о введении Положения в силу и обязательно для ознакомления, соблюдения и исполнения всеми сотрудниками организации.