

Приложение № 7 к Приказу № ____/14-П от «__» _____ 2014 г.

«УТВЕРЖДАЮ»

**Генеральный директор ООО "РЕГИОНАЛЬНЫЙ
ЦЕНТР ДЕНТАЛЬНОЙ ИМПЛАНТАЦИИ И СЛОЖНОГО
ПРОТЕЗИРОВАНИЯ"**

_____/Хамбо В.Е./

«__» _____ 2014 г.

**Положение об организации обработки, информирования,
оформления, учета и хранения персональных данных
пациентов Организации**

Оглавление

1. Общие положения.	3
2. Порядок информирования пациентов об обработке их персональных данных в Организации.....	5
3. Сбор и обработка персональных данных субъектов персональных данных. ...	6
4. Хранение и защита персональных данных субъектов персональных данных.	7
5. Передача персональных данных субъектов ПД.....	8
6. Обязанности субъекта и оператора ПД.....	9
7. Права субъектов в целях защиты персональных данных.	10
8. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта.	11
9. Заключительные положения.	12

1. Общие положения.

Целью настоящего «Положение об организации обработке информирования, оформления, учета и хранения персональных данных» (далее - Положение) является - обеспечение безопасности объектов защиты ООО «РЕГИОНАЛЬНЫЙ ЦЕНТР ДЕНТАЛЬНОЙ ИМПЛАНТАЦИИ И СЛОЖНОГО ПРОТЕЗИРОВАНИЯ» (далее - Организация) от всех видов угроз, внешних и внутренних, умышленных и непредвиденных, минимизация ущерба от возможной реализации угроз безопасности персональных данных, а также обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных пациентов, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

Требования настоящего Положения распространяются на пациентов Организации.

Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных пациентов ООО «РЕГИОНАЛЬНЫЙ ЦЕНТР ДЕНТАЛЬНОЙ ИМПЛАНТАЦИИ И СЛОЖНОГО ПРОТЕЗИРОВАНИЯ», а также ведения их медицинских карт на бумажном и электронном носителях и журналов учета персональных данных пациентов.

Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.06г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.06г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 22.10.04г. № 125-ФЗ «Об архивном деле в Российской Федерации», указанием Федерального агентства по образованию от 22.10.09г. №17-187 «Об обеспечении защиты персональных данных», Федеральным законом РФ от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

В настоящем Положении используются следующие термины и определения:

Оператор персональных данных (далее оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. В рамках настоящего положения оператором является Организация.

Субъект персональных данных - далее субъект, физическое лицо предоставившее оператору свои персональные данные (пациент).

Персональные данные (ПД) - любая информация, относящаяся к определенному или определяемому на её основании физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное положение, место работы, должность, диагноз, другая информация, определяемая нормативно-правовыми актами Российской Федерации, настоящим Положением и приказами Организации.

Обработка персональных данных - действия (операции) с персональными данными, включая систематизацию, накопление, хранение, комбинирование, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Защита персональных данных - деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и обеспечение организационно-технических мер защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения.

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

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.

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

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

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.

2.Порядок информирования пациентов об обработке их персональных данных в Организации.

1) Информирование пациентов осуществляется в целях реализации следующих принципов и положений:

а) [Концепции информационной безопасности.](#)

б) [Политики информационной безопасности.](#)

2) Перечень персональных данных подлежащих обработке определен в Перечне сведений конфиденциального характера, обрабатываемых в Организации.

3) Информирование осуществляется по запросам (обращениям) пациентов в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. законов от 25.11.2009 № 266-ФЗ и от 27.12.2009 № 363-ФЗ) (далее Закон 152-ФЗ).

4) Список лиц, имеющих доступ к персональным данным пациентов определен в «Положение о разграничении прав доступа к обрабатываемым персональным данным персональным данным в информационных системах персональных данных в Организации»

5) Обращение пациентов отражаются и фиксируются в Журнале учета обращений и информирования пациентов об обработке их ПДн.

6) По каждому случаю обращения (запроса) пациента должна быть сделана запись о факте его информирования (ответе).

3. Сбор и обработка персональных данных субъектов персональных данных.

Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Сбор и обработка персональных данных пациентов осуществляется исключительно с письменного согласия субъекта. Образцы форм заявления о согласии на обработку персональных данных и отказа от нее, находятся на стойке администратора, заполняются в первую очередь и вклеиваются в медицинскую карту пациента. Персональные данные субъекта ПД относятся к конфиденциальной информации.

В целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных субъекта ПД обязаны соблюдать следующие общие требования:

1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, наблюдения и лечения пациентов и обеспечения сохранности имущества оператора, пациента и третьих лиц.

2. Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

3. Информация о персональных данных субъекта предоставляется оператору субъектом устно или иным удобным для субъекта способом. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

4. Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений.

5. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

При обращении в Организацию пациент представляет следующие документы, содержащие персональные данные о себе:

паспорт или иной документ, удостоверяющий личность;

полис(карта) ДМС (гарантийное письмо, иной документ от страховой организации).

4. Хранение и защита персональных данных субъектов персональных данных.

Персональные данные субъектов хранятся на электронных и бумажных носителях. Бумажные носители хранятся в помещении у администратора. Для этого используются специально оборудованные шкафы или сейфы. Медицинские карты субъектов, прошедших обследование и лечение, хранятся в архиве организации или администратора.

Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

Конкретные обязанности по ведению, заполнению медицинских карт субъектов, иных документов, отражающих персональные данные пациентов, возлагается на администрацию, врачебный и средний медицинский персонал, а по хранению медицинских карт обследованных, пролеченных субъектов - на администраторов.

При получении сведений, составляющих персональные данные субъектов, заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий в рамках должностных инструкций.

Защита персональных данных пациентов в Организации возлагается на:

1. главного врача;
2. администраторов;
3. администратора компьютерной сети (программиста);
4. юрисконсульта;
5. медицинский персонал.

Администратор компьютерной сети (программист) обеспечивает следующие меры по защите, хранящейся на сервере информации:

1. ограничение сетевого доступа на сервер для определенных пользователей;
2. организацию контроля технического состояния серверов и уровней защиты и восстановления информации;
3. проведение регулярного резервного копирования информации;
4. ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации.

Работники Организации, имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

5. Передача персональных данных субъектов ПД.

При передаче персональных данных субъектов работники Организации, имеющие доступ к персональным данным, должны соблюдать следующие требования:

1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия работника субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных федеральными законами. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора, отсутствует угроза жизни или здоровью субъекта, оператор обязан отказать в предоставлении персональных данных лицу.

2. Предупредить лиц, получающих персональные данные субъекта, 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.

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

4. Все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

6. Обязанности субъекта и оператора ПД.

В целях обеспечения достоверности персональных данных субъект обязан предоставить оператору необходимые данные.

Оператор обязан:

1. Осуществлять защиту персональных данных субъектов.
2. Обеспечить хранение учетной и медицинской документации. При этом 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.
3. Субъекты или их законные представители должны быть ознакомлены под расписку с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.
4. Все работники, имеющие доступ к персональным данным пациентов, обязаны ознакомиться и подписать соглашение о неразглашении персональных данных.

7. Права субъектов в целях защиты персональных данных.

В целях обеспечения защиты персональных данных, хранящихся у оператора, субъекты имеют право на:

1. Полную и безвозмездную информацию об их персональных данных и обработке этих данных.
2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом.
3. Определение своих представителей для защиты своих персональных данных.
4. Требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.
5. Обжалование в суде любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

8. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

9.Заключительные положения.

Настоящее Положение вступает в силу с момента его утверждения генеральным директором Организации.

Настоящее Положение доводится до сведения всех субъектов ПД.

Настоящее Положение доводится до сведения всех работников Организации.