

ПОЛОЖЕНИЕ
О порядке обработки и обеспечении безопасности
персональных данных пациентов Акционерного общества
«Стоматологическая поликлиника №4»

1. Общие положения

1.1. Настоящее Положение о порядке обработки и обеспечении безопасности персональных данных (далее ПДн) пациентов в Акционерном обществе «Стоматологическая поликлиника №4» (далее – Положение) разработано в соответствии с: Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее - Федеральным законом); постановлением Правительства Российской Федерации от 15 сентября 2008 г. №678 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Приказом ФСТЭК № 21 от 18 февраля 2013 г. «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; Конституции Российской Федерации; Трудового кодекса Российской Федерации и устанавливает единый порядок обработки персональных данных в акционерном обществе «Стоматологическая поликлиника №4» (далее – Общество).

1.2. В настоящем Положении используются следующие термины и определения:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или кругу лиц;
- 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;
- 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;
- 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;
- информационная система персональных данных (далее ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;
- технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и

системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- работник Общества – лицо, допущенное к обработке ПДн пациентов.

1.3. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к ПДн пациентов.

1.4. Настоящее Положение разработано с целью – защиты ПДн пациентов, обращающихся за медицинской помощью в Общество.

1.5. Целью обработки ПДн пациентов в Обществе является оказание медицинской помощи конкретному пациенту.

1.6. Настоящее Положение и изменения к нему утверждаются Главным врачом Общества и вводятся приказом по Обществу. Положение в обязательном порядке доводится до работников Общества допущенных к обработке ПДн пациентов под роспись.

2. ПДн пациентов обрабатываемых в Обществе

2.1. Перечень ПДн: перечень персональных данных пациентов обратившихся в Общество за медицинской помощью представлен в табл. 1.

Таблица 1

№ п/п	Наименование (вид) ПДн	Содержание ПДн	Источник получения	Основание для обработки ПДн	Срок хранения, условия прекращения обработки
1	Первичные учетные данные пациентов	ФИО пациента	Субъект ПДн	- согласие субъекта на обработку его ПДн	
2	Сведения о реквизитах пациента	- дата рождения; - место и дата рождения; - адрес постоянной регистрации; - паспортные данные; - контактная информация; - социальное положение; - гражданство.	Субъект ПДн	- согласие субъекта на обработку его ПДн	
3	Дополнительные сведения о пациенте	- оказанные услуги.	Субъект ПДн	- согласие субъекта на обработку его ПДн	

3. Основные условия проведения обработки ПДн в Обществе

3.1. Обработка ПДн осуществляется:

- после направления уведомления об обработке ПДн в Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Пермскому краю;
- после принятия необходимых мер по защите ПДн пациентов в Обществе.

4. Порядок определения защищаемой информации в Обществе

4.1. В Обществе защищаемая информация, отнесенная к ПДн, определяется на основании следующих разработанных документов:

- Перечнем персональных данных, подлежащих защите в информационной системе персональных данных акционерного общества «Стоматологическая поликлиника №4»;
- настоящим Положением и Политикой обработки и защиты персональных данных.

5. Допуск к ПДн пациентов

Допуск к работе с ПДн пациентов осуществляется на основании разработанного документа в Обществе «Перечень подразделений и работников акционерного общества «Стоматологическая поликлиника №4» допущенных к работе с персональными данными в информационной системе персональных данных акционерного общества «Стоматологическая поликлиника №4».

6. Порядок получения ПДн пациента работником Общества для дальнейшей обработки

Работник Общества получает информацию, относящуюся к ПДн пациентов для ее дальнейшей обработки следующими законными способами:

- при личном контакте с пациентом (или его ближайшего окружения). Пациент (ближайшее окружение) лично представляет свои (его) ПДн работнику Общества (регистратура) на бумажном носителе.

7. Обработка и хранение ПДн пациента

7.1. Обработка ПДн пациента в ИСПДн Обществе с использованием средств автоматизации.

7.1.1. Не допускается обработка ПДн пациента в ИСПДн с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации ИСПДн, включающих Акт классификации ИСПДн, инструкции пользователю по организации антивирусной защиты, и других нормативно методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации в обществе;
- разработанных организационных мер по защите обработки ПДн в помещениях, предназначенных для их обработки, расположенном на в административном здании Общества.

7.1.2. По достижению цели обработки ПДн пациентов, которые не будут использоваться в дальнейшем, должны быть удалены из ИСПДн в срок не превышающей 30-ти дней с даты достижения цели обработки ПДн.

7.2. Обработка ПДн пациентов без использования средств автоматизации.

7.2.1. Неавтоматизированная обработка ПДн пациентов осуществляется в Обществе в виде документов на бумажных носителях, в соответствии с принятыми установленными формами в Обществе. Запись работником ПДн пациентов на съемные носители (флеш память, магнитные диски и т.д.) осуществляется в случае необходимости в целях резервного копирования.

7.2.1.1. При неавтоматизированной обработке ПДн пациентов в Обществе на бумажных носителях должны соблюдаться следующие правила:

- не допускается фиксация на одном бумажном носителе (в соответствии с установленными формами) ПДн, цели, обработки которых заведомо не совместимы;
- ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях;

- документы, содержащие ПДн на бумажных носителях должны храниться в систематизированном виде в служебных помещениях Общества отдельно от других документов только в надежно запираемых и опечатываемых шкафах (сейфах);

- бумажные носители, содержащие ПДн, достигшие цели своей обработки уничтожаются в присутствии специально созданной комиссии с составлением Акта об уничтожении носителей ПДн (форма Акта уничтожения Приложение №1);

7.2.1.2. Пациент либо его законный представитель имеет право по запросу, направленному в том числе в электронной форме, получать отражающие состояние здоровья пациента медицинские документы (их копии) и выписки из них, в том числе в форме электронных документов. Порядок и сроки предоставления медицинских документов (их копий) и выписок из них устанавливаются уполномоченным федеральным органом исполнительной власти.

8. Защита ПДн пациентов

8.1. Защита ПДн пациентов в Обществе организована в соответствии с разработанными и введенными организационными и техническими мерами защиты, которые доводятся до каждого работника Общества допущенного к обработке ПДн пациентов под роспись. В дополнение к разработанным вышеперечисленным мерам в Обществе введены следующие правила по защите ПДн пациентов, а именно:

- в целях обеспечения сохранности и конфиденциальности ПДн пациентов в Обществе все операции должны выполняться только уполномоченными на эти действия сотрудниками: Директором Общества, сотрудниками регистратуры, осуществляющие данную обработку в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях, лечащими врачами.

10. Права пациентов

Пациент имеет право:

10.1. Запретить обработку своих ПДн в Обществе.

11. Ответственность за разглашение информации отнесенной к ПДн пациента

11.1. Лица виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн пациента, несут предусмотренную законодательство Российской Федерации ответственность.

Приложения

Приложение №1. Акт уничтожения носителей ПДн

УТВЕРЖДАЮ

Главный врач

«Стоматологическая поликлиника №4»

« » _____ 201_ г.
М П

A K T №

об уничтожении носителей персональных данных

Комиссия, в составе:

Председатель: _____ /

Члены комиссии: _____ / _____ /
 _____ / _____ /

провела отбор носителей персональных данных (бумажные носители, съемные носители) и установила, что в соответствии с требованиями руководящих документов по защите информации отнесенной к персональным данным, информация, записанная на этих носителях, достигла цели своей обработки и подлежит дальнейшему уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя персональных данных	Примечание
1				
2				
3				

После утверждения акта персональные носители сверены с записями в акте и уничтожены путем

(разрезание, сжигание, механическое уничтожение и т.п.)

Уничтоженные носители с журналов учета списаны.

Подписи членов комиссии:

Председатель: _____ /

Члены комиссии: _____ / _____ /
 _____ / _____ /

С положением ознакомлен(а):

Должность _____

Дата, подпись

ФИО

[illegible]