ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО ДПО «Академия практической медицины «Абилити»

Настоящая политика в отношении обработки и защиты персональных данных (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и является основополагающим внутренним медицинской организации, определяющим ключевые направления его деятельности в области обработки и защиты персональных данных.

Политика разработана в целях реализации требований законодательства и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в медицинской организации, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

Цель обработки персональных данных

Целью обработки, включая сбор, запись, систематизацию, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, является оказание медицинских услуг и исполнение обязательств организации перед пациентом по договору с ним, связь с пациентом в случае необходимости, а также выполнение условий трудового договора с работниками организации в соответствии с действующим законодательством.

Принципы обработки персональных данных

При обработке персональных данных медицинская организация придерживается следующих принципов:

соблюдение законности получения, обработки, хранения, а так же других действий с персональными данными;

обработка персональных данных исключительно с целью исполнения своих обязательств по договору оказания услуг, а также по трудовому договору;

сбор только тех персональных данных, которые минимально необходимы для достижения заявленных целей обработки;

выполнение мер по обеспечению безопасности персональных данных при их обработке и хранении;

соблюдение прав субъекта персональных данных на доступ к его персональным данным;

соответствие сроков хранения персональных данных заявленным целям обработки.

Конфиденциальность персональных данных

Работники медицинской организации и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Состав персональных данных

В состав обрабатываемых в компании персональных данных пациентов и работников могут входить:

фамилия, имя, отчество;

пол;

дата рождения или возраст;

паспортные данные ;

адрес проживания;

номер телефона, факса, адрес электронной почты (по желанию);

информация о состоянии здоровья;

другая информация, необходимая для правильного проведения и интерпретации медицинских исследований;

результаты выполненных медицинских исследований;

другая информация, необходимая для выполнения обязательств организации в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, законодательством об обязательных видах страхования, со страховым законодательством.

Медицинская организация осуществляет обработку данных о состоянии здоровья пациентов в целях оказания медицинских услуг, установления медицинского диагноза при этом обработка персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Организация осуществляет обработку данных о состоянии здоровья работников организации в соответствии с трудовым законодательством Российской Федерации.

Сбор (получение) персональных данных

Персональные данные пациентов организация получает только лично от пациента или от его законного представителя. Персональные данные пациента могут быть получены с его слов и не проверяются.

Обработка персональных данных

Обработка персональных данных в организации происходит как неавтоматизированным, так и автоматизированным способом.

К обработке персональных данных в организации допускаются только сотрудники прошедшие определенную процедуру допуска, к которой относятся:

ознакомление сотрудника с локальными нормативными актами организации (положения, инструкции и т.д.), строго регламентирующими порядок и процедуру работы с персональными данными;

взятие с сотрудника подписки о соблюдении конфиденциальности в отношении персональных данных при работе с ними.

получение сотрудником и использование в работе индивидуальных атрибутов доступа к информационным системам компании, содержащим в себе персональные данные. При этом каждому сотруднику выдаются минимально необходимые для исполнения трудовых обязанностей права на доступ в информационные системы.

Сотрудники, имеющие доступ к персональным данным, получают только ту информацию, которая необходима им для выполнения конкретных трудовых функций.

Хранение персональных данных

Персональные данные пациентов хранятся в бумажном (амбулаторная карта, бланки направлений, результаты обследований) и электронном виде. В электронном виде персональные данные пациентов хранятся в информационной системе персональных данных организации, а так же в архивных копиях баз данных этих систем. Порядок архивирования и сроки хранения архивных копий баз данных информационной системы персональных данных организации определены в инструкции о резервном копировании, которая является обязательной для исполнения администраторами соответствующей системы.

При хранении персональных данных пациентов и работников соблюдаются организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним.

К ним относятся:

назначение сотрудника ответственного за тот или иной способ хранения персональных данных;

ограничение физического доступа к местам хранения и носителям;

учет всех информационных систем и электронных носителей, а так же архивных копий.

Передача персональных данных третьим лицам

Передача персональных данных третьим лицам возможна в исключительных случаях только с согласия пациента и только с целью исполнения обязанностей перед пациентом в рамках

оказания услуг, кроме случаев, когда такая обязанность у организации наступает в результате требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов. В данном случае компания ограничивает передачу персональных данных запрошенным объемом.

Персональные данные пациента (в том числе результаты исследований) могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента, за исключением случаев, когда передача персональных данных без его согласия допускается действующим законодательством РФ. В качестве такого разрешения могут выступать:

нотариально заверенная доверенность;

собственноручно написанная клиентом доверенность в присутствии сотрудника медицинской организации и им заверенная.

Меры по обеспечению безопасности персональных данных при их обработке

Обеспечение безопасности персональных данных в организации достигается следующими мерами:

назначением сотрудника, ответственного за организацию обработки персональных данных;

проведением внутреннего аудита информационной системы организации, содержащей персональные данные, проведением их классификации;

разработкой частной модели угроз безопасности персональных данных;

определением списка лиц, допущенных к работе с персональными данными;

разработкой и утверждением локальных нормативных актов организации, регламентирующих порядок обработки персональных данных. Разработкой для администраторов информационной системы рабочих инструкций;

реализацией технических мер, снижающих вероятность реализаций угроз безопасности персональных данных;

проведением периодических проверок состояния защищенности информационной системы организации.

Права пациента

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

подтверждение факта обработки персональных данных;

правовые основания и цели обработки персональных данных;

цели и применяемые способы обработки персональных данных;

сведения о лицах (за исключением работников организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании федерального закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных своих прав;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению организации, если обработка поручена или будет поручена такому лицу.

Соответствующая информация предоставляется субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен быть составлен в соответствии с требованиями законодательства.