

Приложение № 5
к приказу Директора ФГУП
«Брянское ПрОП» Минтруда
России
от «__» _____ 2014г. № __.

**Политика обработки персональных данных
Федерального государственного унитарного предприятия «Брянское
протезно-ортопедическое предприятие» Министерства труда и
социальной защиты Российской Федерации**

Брянск 2014

Общие положения

Федеральное государственное унитарное предприятие «Брянское протезно-ортопедическое предприятие» Министерства труда и социальной защиты Российской Федерации (далее – Организация) осуществляет свою деятельность в соответствии с действующим законодательством Российской Федерации по направлениям, обозначенным в полученных лицензиях на осуществление медицинской деятельности. Оказание медицинских услуг предполагает смешанную обработку и хранение персональных данных пациентов. В соответствии с действующим законодательством Организация выполнила комплекс технических и организационных мероприятий для обеспечения безопасности обрабатываемых и хранимых персональных данных.

Одна из приоритетных задач в работе Организации - соблюдение действующего законодательства Российской Федерации в области информационной безопасности, а также требований федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных», основной целью которого является 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.

Цель обработки персональных данных

Целью обработки, включая сбор, запись, систематизацию, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных, является оказание медицинских услуг и исполнение обязательств Организации перед пациентом по договору с ним (обязательное медицинское страхование, добровольное медицинское страхование, договор на платное медицинское обслуживание), связь с пациентом в случае необходимости, выполнение условий трудового договора с работниками Организации в соответствии с действующим

законодательством, а также осуществление пропускного режима на территорию Организации.

Принципы обработки персональных данных

При обработке персональных данных Организация соблюдает следующие принципы:

- соблюдение законности получения, обработки, хранения, а также 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 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 Организации персональных данных пациентов и работников могут входить: дата рождения;

– адрес места проживания;

- место работы (учебы);
- данные документа, удостоверяющего личность;
- СНИЛС;
- диагноз;
- анамнез;
- инвалидность;
- заказы;
- справка МСЭК;
- сведения о медицинском работнике или медицинских работников, оказавших медицинскую услугу;
- другая информация, необходимая для выполнения обязательств учреждения 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.

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 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.

Обработка персональных данных

Обработка персональных данных в Организации происходит смешанным способом.

К обработке персональных данных 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 Организации, 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 (договор, согласие на обработку персональных данных, амбулаторная карта, бланки направлений, результаты обследований) и электронном виде. В электронном виде персональные данные пациентов хранятся в информационных системах персональных данных Организации «Учет, обеспечение ПОИ и медицинскими услугами» и «Мед-Комплит», а также в их архивных копиях. 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 персональных данных;
- учет всех информационных систем и электронных носителей, а также 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 договора оказания услуг, кроме случаев, когда такая обязанность у организации наступает в результате требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов.

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 информационных систем организации, содержащих персональные данные, проведением их классификации;
- разработкой модели угроз безопасности персональных данных;
- определением списка лиц, допущенных к работе с персональными данными;
- разработкой и утверждением локальных нормативных актов Учреждения, 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 учреждения.

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.