Приложение 1
к приказу №22 от 09.01.2020

Политика
обработки персональных данных
в ООО «Медсервис Профи»

1. Общие положения

1.1. Политика обработки персональных данных (далее – Политика) в ООО «Медсервис Профи» сформирована с целью соблюдения требований законодательства Российской Федерации в сфере обработки персональных данных.

1.2. Политика определяет основные принципы и направления работы в области обработки персональных данных в медицинской организации.

1.3. Политика определена в соответствии со следующими нормативными правовыми актами РФ:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральным законом от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- а так же в соответствии с иными нормативно-правовыми актами, регламентирующими деятельность в сфере обработки персональных данных.

2.Основные понятия

2.1.В целях реализации настоящей Политики используются следующие основные понятия:

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Оператор – медицинская организация самостоятельно или совместно с другими лицами организующая и (или) осуществляющая обработку персональных данных, а также определяющая 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;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их

обработку информационных технологий и технических средств;

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Категории субъектов персональных данных, обработка персональных данных которых осуществляется

3.1.Оператором осуществляется обработка персональных данных у следующих категорий субъектов персональных данных:

- сотрудников медицинской организации;

- пациентов медицинской организации.

4.Принципы обработки персональных данных в медицинской организации

4.1.Обработка персональных данных осуществляется на законной и справедливой основе.

4.2.Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.3.Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.4.Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.5.Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.6.При обработке персональных данных должны быть обеспечены

точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

4.7.Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.Условия обработки персональных данных в медицинской организации

5.1.Оператор в своей деятельности обеспечивает соблюдение условий обработки персональных данных, установленных Федеральным законом № 152-ФЗ «О персональных данных».

5.2.Оператор не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений.

5.3.Оператор не производит трансграничную (на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

6.Меры по обеспечению безопасности персональных данных при их обработке

6.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении

персональных данных.

6.2. Обеспечение безопасности персональных данных достигается, в том числе:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных законодательству о персональных данных, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

- оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных, соотношением указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных

законодательством о персональных данных;

- а так же иными мерами, предусмотренными законодательством.

7.Регулирование обработки персональных данных в медицинской организации локальными нормативными актами

7.1. В целях соблюдения установленных законодательством Российской Федерации требований к обработке персональных данных медицинская организация принимает необходимые локальные нормативные акты.

7.2. Медицинская организация принимает локальные нормативные акты по вопросам обработки персональных данных, а также локальные нормативные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации по вопросам обработки персональных данных, устранение последствий таких нарушений.

7.3.Руководителем медицинской организации принимаются локальные нормативные акты о допуске к обработке персональных данных, а так же определяющие ответственность работников, допущенных к обработке персональных данных.

8.Права и обязанности при обработке персональных данных

8.1.При обработке персональных данных в медицинской организации соблюдаются права и обязанности, установленные действующим законодательством.

8.2. При обработке персональных данных соблюдаются следующие права субъекта персональных данных:

- право субъекта персональных данных на доступ к его персональным данным;

- права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации;

- права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных

данных;

- право на обжалование действий или бездействия оператора;

- а также иные права, установленные действующим законодательством.

8.3. При обработке персональных данных оператор соблюдает выполнение следующих обязанностей:

- обязанности оператора при сборе персональных данных;

- меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

- меры по обеспечению безопасности персональных данных при их обработке;

- обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных;

- обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

- а также иные обязанности, установленные действующим законодательством.

9. Заключительные положения

9.1.Политика вступает в законную силу с момента утверждения её руководителем организации и действует до утверждения новой.

9.2.Настоящая Политика доводится до сведения субъектов персональных данных, обработка персональных данных которых осуществляется Оператором.

9.3. Лица, виновные в нарушении требований законодательства в области персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.