УТВЕРЖДЕНО
Директор ООО «ЗДОРОВЬЕ ФЕОДОСИЯ»

_____Баранин А.В.

от «15» октября 2019 г.

**Положение об обработке персональных данных клиентов и контрагентов ООО «ЗДОРОВЬЕ ФЕОДОСИЯ»**

1. **1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Положение об обработке персональных данных клиентов и контрагентов (далее – Положение) определяет порядок обработки и защиты персональных данных (далее – ПДн) клиентов и контрагентов **ООО «ЗДОРОВЬЕ ФЕОДОСИЯ»** (далее именуется – Учреждение).

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», Постановлениями Правительства РФ от 15.09.2008 №687 и от 01.11.2012 № 1119 и иными нормативными актами, действующими на территории Российской Федерации.

1.3. Действие настоящего Положения распространяется на всех работников Учреждения и доводится до их сведения, персонально под роспись.

1.4. Настоящее Положение вступает в силу со дня его утверждения. Все изменения в настоящее Положение вносятся Приказом Учреждения.

1.5. Контроль за выполнением настоящего Положения возлагается на заместителя директора по медицинской части Учреждения.

1.6. В настоящем Положении используются следующие термины и определения:

**Учреждение** – Оператор, осуществляющий обработку ПДн, а также определяющий цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн клиентов и контрагентов. Клиент/Контрагент – физическое лицо, официальный представитель – физическое лицо юридического лица и/или индивидуального предпринимателя, вступившее в договорные отношения по оказанию услуг с Учреждением.

**Персональные данные Клиента/Контрагента** – ПДн, необходимые Учреждению в связи с исполнением договорных отношений и касающиеся конкретного Клиента/Контрагента, в том числе его фамилия, имя, отчество, фамилия при рождении, год, месяц, дата и место рождения, адрес места жительства, данные об общегражданском паспорте Российской Федерации (серия и номер общероссийского паспорта, дата его выдачи, наименование органа, выдавшего паспорт - срок действия общероссийского паспорта) либо свидетельства о рождении, копии общегражданских паспортов Клиентов, копии

правоустанавливающих документов, являющихся предметом договорных отношений, адрес регистрации, адрес электронной почты, домашний и контактный (мобильный) телефоны.

**Обработка ПДн** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение ПДн.

**Защита ПДн Клиента/Контрагента** – деятельность Учреждения по обеспечению с помощью локального регулирования порядка обработки ПДн и организационно-технических мер обеспечения конфиденциальности информации, защиты от уничтожения, изменения, блокирования.

**Конфиденциальность ПДн** – обязательное для соблюдения лицом, получившим доступ к ПДн, требование не допускать их распространения и передачи третьим лицам без согласия субъекта ПДн или наличия иного законного основания.

## 2. 2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. ПДн Клиента/Контрагента относятся к категории конфиденциальной информации. Учреждение обеспечивает конфиденциальность персональных данных, и обязано не допускать их распространения без согласия Клиента/Контрагента, либо наличия иного законного основания.

2.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Клиента/Контрагента распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

2.3. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем по которому является Клиент/Контрагент, а также для заключения договора по инициативе Клиента/Контрагента или договора, по которому Клиент/Контрагент будет являться выгодоприобретателем;

2.4. Обработка персональных данных Клиента/Контрагента необходима для соблюдения прав и законных интересов Учреждения или иных третьих лиц при соблюдении условия, что при этом не нарушаются права и свободы Клиента/Контрагента.

2.5. Обработка персональных данных Учреждением в интересах Клиента/Контрагента заключается в получении, систематизации, накоплении, хранении, уточнении (обновлении, изменении), использовании, обезличивании, блокировании, уничтожении и в защите от несанкционированного доступа персональных данных Клиентов/Контрагентов.

2.6. Обработка персональных данных Клиентов/Контрагентов ведется методом смешанный (в том числе автоматизированной) обработки.

2.7. В целях обеспечения прав и свобод человека и гражданина Учреждение и его представители при обработке ПДн Клиента/Контрагента соблюдают следующие общие требования:

2.7.1. Обработка ПДн Клиента/Контрагента осуществляется для выполнения функций, полномочий и обязанностей, возложенных на Учреждение уставом.
2.7.2. При определении объема и содержания обрабатываемых ПДн Клиента/Контрагента Учреждение руководствуется законодательством Российской Федерации.
2.7.3. Все ПДн Клиента/Контрагента Учреждение получает у него самого, за исключением случаев, когда их получение возможно только у третьей стороны способом, не противоречащим законодательству Российской Федерации.
2.7.4. Обработка ПДн, полученных от третьих лиц, возможна только при уведомлении субъекта ПДн.
2.7.5. Учреждение не получает и не обрабатывает ПДн Клиента/Контрагента о его политических, религиозных и иных убеждениях и частной жизни.
2.7.6. ПДн не используются в целях причинения какого-либо ущерба (вреда) Клиенту/Контрагенту, затруднения реализации его прав и свобод.
2.7.7. При принятии решений, затрагивающих интересы Клиента/Контрагента, Учреждение не основывается на ПДн Клиента/Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.
2.8. При идентификации Представителя Клиента/Контрагента Учреждение требует предъявление документов, удостоверяющих личность и подтверждающих полномочия представителя.
2.9. При заключении договора, как и в ходе его исполнения, может возникнуть необходимость в предоставлении Клиентом/Контрагентом иных документов, содержащих информацию о нем.
2.10. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, ПДн Клиента/Контрагента, так же будут включены в договоры, включение в которые персональных данных Клиента/ Контрагента необходимо согласно действующему законодательству Российской Федерации.
2.11. Согласие Представителя субъекта на обработку его персональных данных дается в форме конклюдентных действий, выраженных в предоставлении доверенности на право действовать от имени и по поручению субъектов персональных данных, и документа, удостоверяющего его личность.
2.12. Согласие субъектов на предоставление их персональных данных не требуется при получении Учреждением, в рамках установленных полномочий, мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, а также органов власти и местного самоуправления, налоговых органов, судебных приставов, иных организаций, направляющих в Учреждение запросы по подтверждению наличия/отсутствия факта гражданско-правовых отношений между Учреждением и Клиентом/Контрагентом( при оказании услуг либо трудовых отношениях).
Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия

органа, направившего запрос, а также перечень запрашиваемой информации. В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, Учреждение обязано получить согласие субъекта ПДн на предоставление его персональных данных и предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено.

## 3. 3. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Защита ПДн Клиентов/Контрагентов, обрабатываемых Учреждением, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных. Правовые меры включают:

- разработку локальных актов Учреждения, реализующих требования Российского законодательства, в том числе политики в отношении обработки персональных данных, и размещение ее на интернет-сайте Учреждения;
- отказ от любых способов обработки персональных данных, не соответствующих целям, заранее предопределенным Учреждением;
- оценку вреда, который может быть причинен ПДн Клиентов/Контрагентов в случае нарушения требований Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством.

Организационные меры включают:

- назначение лиц, ответственных за организацию обработки ПДн Клиентов/Контрагентов;
- назначение лица, ответственного за обеспечение безопасности ПДн Клиентов/Контрагентов в информационных системах;
- осуществление внутреннего контроля обработки персональных данных требованиям Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн Клиентов/Контрагентов, определенным в политике и локальных актах Учреждения;
- ограничение состава работников, имеющих доступ к ПДн Клиентов/Контрагентов, и организацию разрешительной системы доступа к ним;
- ознакомление работников с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, с локальными актами Учреждения по вопросам обработки персональных данных;
- обучение всех категорий работников, непосредственно осуществляющих обработку ПДн Клиентов/Контрагентов, правилам работы с ними и обеспечения безопасности обрабатываемых данных;
- определение в должностных инструкциях работников обязанностей по обеспечению безопасности обработки ПДн Клиентов/Контрагентов и ответственности за нарушение установленного порядка;

- регламентацию процессов обработки персональных данных;
- организацию учёта материальных носителей ПДн Клиентов/Контрагентов, их хранения, обеспечивающую предотвращение хищения, подмены, несанкционированного копирования и уничтожения;
- определение типа угроз безопасности ПДн Клиентов/Контрагентов, актуальных для информационных систем персональных данных с учетом оценки возможного вреда субъектам персональных данных, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности персональных данных, формирование частных моделей актуальных угроз ПДн Клиентов/Контрагентов;
- размещение технических средств обработки ПДн Клиентов/Контрагентов в пределах охраняемой территории;
- ограничение допуска посторонних лиц в помещения Учреждения, недопущение их нахождения в помещениях, где ведется работа с ПДн Клиентов/Контрагентов и размещаются технические средства их обработки, без контроля со стороны работников Учреждения.

Технические меры включают:
- реализацию разрешительной системы доступа работников к ПДн Клиентов/Контрагентов, обрабатываемым в информационных системах, и программно-аппаратным и программным средствам защиты информации;
- выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Учреждения, обеспечивающих соответствующую техническую возможность;
- обеспечение безопасности среды виртуализации;
- безопасное межсетевое взаимодействие (применение межсетевого экранирования);
- обнаружение вторжений в информационную систему Учреждения, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (использование системы резервного копирования и восстановления персональных данных);
- периодическое проведение мониторинга действий пользователей, разбирательств по фактам нарушения требований безопасности персональных данных;
- контроль за выполнением указанных выше требований не реже 1 раза в 3 года.

3.2. Все работники, имеющие доступ к ПДн Клиентов/Контрагентов, подписывают Обязательство о неразглашении персональных данных.

3.3. Защита ПДн Клиентов/Контрагентов от неправомерного их использования или утраты обеспечивается Учреждением в порядке, установленном законодательством Российской Федерации, внутренними регламентирующими документами Учреждения.

3.4. Защите подлежат: ПДн Клиентов/Контрагентов на бумажных носителях; материальные носители информации, содержащие ПДн Клиентов/Контрагентов.
3.5. Ответственные лица структурных подразделений Учреждения, хранящих ПДн на бумажных и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования на местах.
3.6. Ответственные лица, обрабатывающие ПДн на бумажных носителях, в информационных системах ПДн и на машинных носителях информации, обеспечивают защиту в соответствии с требованиями законодательства Российской Федерации, нормативными и методическими документами, касающимися защиты ПДн.
3.7. Ответственность за организацию данных процессов несут все работники Учреждения, непосредственно осуществляющие работу по обработке и хранению ПДн Клиентов/Контрагентов.
3.8. Работник Учреждения, имеющий доступ к персональным данным Клиентов/Контрагентов в связи с исполнением трудовых обязанностей:
- обеспечивает хранение информации, содержащей персональные данные Клиента, исключающее доступ к ним третьих лиц.
- в отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные Клиентов/Контрагентов.
- при уходе в отпуск, во время служебной командировки и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные Клиентов/Контрагентов лицу, на которое локальным актом Учреждения (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные Клиентов/Контрагентов, передаются заместителю директора Учреждения.
- при увольнении работника, имеющего доступ к персональным данным Клиентов/Контрагентов, документы и иные носители, содержащие персональные данные Клиентов/Контрагентов, передаются другому работнику, имеющему доступ к персональным данным Клиентов/Контрагентов по указанию директора Учреждения.
3.9. Защита доступа к электронным носителям, содержащим персональные данные Клиентов/Контрагентов, обеспечивается, в том числе:
- организацией контроля доступа в помещения информационной системы посторонних лиц;
- использованием лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный доступ к персональным данным;
- разграничением прав доступа с использованием учетной записи.
- 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.

- учетом машинных носителей персональных данных.
- обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.
- контролем эффективности принимаемых мер по обеспечению защищенности персональных данных.

3.10. Ответы на письменные запросы других организаций и учреждений о персональных данных Клиентов/Контрагентов даются только с письменного согласия самого Клиента/Контрагента, если иное не установлено законодательством. Ответы оформляются в письменном виде, на бланке Учреждения, и в том объеме, который позволяет не разглашать излишний объем персональных данных Клиента/Контрагента.

## 4. 4. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сведения о Клиентах/Контрагентах на бумажных носителях хранятся в помещениях Учреждения. Для хранения носителей используются специально оборудованные закрывающиеся шкафы (ящики), расположенные внутри контролируемых зон Учреждения.

4.2. Обязанности по хранению документов, в которых содержатся ПДн Клиентов/Контрагентов, возлагаются на руководителей структурных подразделений Учреждения, в которых обрабатывается информация.

4.3. Ключи от шкафов (ящиков), в которых хранятся носители ПДн, находятся у сотрудника, обрабатывающего данную информацию.

4.4. ПДн Клиентов/Контрагентов могут также храниться в электронном виде, доступ к которым ограничен.

4.5. Доступ к ПДн Клиентов/Контрагентов без специального разрешения имеют сотрудники, занимающие в Учреждении следующие должности:
- директор;
- главный врач;
- главный бухгалтер.

4.6. Внутренний доступ к ПДн Клиентов/Контрагентов другим работникам Учреждения может быть предоставлен только лицам, внесенным в Список лиц, допущенных к обработке ПДн и только в интересах и в объеме выполнения ими должностных обязанностей.

4.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.8. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию при поступлении соответствующего заявления, если иное не предусмотрено законодательством.

4.9. По истечении срока действия документов, содержащих ПДн, они должны быть уничтожены с соблюдением Правил уничтожения. Работник, отвечающий за уничтожение документов, содержащих ПДн, несет персональную ответственность за их неразглашение.

4.10. Результатом уничтожения ПДн должна стать невозможность восстановить содержание ПДн в информационной системе ПДн и (или) на материальных носителях.

## 5. 5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При передаче ПДн Клиента/Контрагента соблюдаются следующие требования, и выполняются следующие условия:

5.1.1. Учреждение осуществляет обработку ПДн Клиента/Контрагента в пределах своей организации в соответствии с настоящим Положением.

5.1.2. Учреждение разрешает доступ к ПДн Клиентов/Контрагентов только специально уполномоченным лицам, при этом указанные лица вправе получать только те ПДн Клиента/Контрагента, которые необходимы для выполнения конкретных функций.

5.1.3. Учреждение вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законодательством, с согласия субъекта ПДн.

5.1.4. В случае если Учреждение поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку ПДн по поручению Учреждения, несет ответственность перед Учреждением.

5.1.5. Учреждение передает ПДн Клиента/Контрагента его представителям в порядке, установленном законодательством Российской Федерации, и ограничивает эту информацию только теми персональными данными Клиента или Контрагента, которые необходимы для выполнения указанными представителями их функций.

5.2. Все сведения о передаче ПДн Клиентов/Контрагентов регистрируются в Журнале учета передачи ПДн в целях контроля правомерности использования данной информации лицами, ее получившими. В Журнале фиксируются сведения о лице, направившем запрос, дата передачи ПДн или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана. Регистрацию действий по передаче и/или обращений субъектов ПДн осуществляют Лица, ответственные за организацию обработки ПДн (в рамках направлений деятельности).

## 6. 6. ОБЯЗАННОСТИ КЛИЕНТА/КОНТРАГЕНТА И УЧРЕЖДЕНИЯ

6.1 Клиент/Контрагент обязан:

6.1.1. При заключении договора предоставить Учреждению полные и достоверные данные о себе.

6.1.2. В случае изменения сведений, составляющих ПДн Клиента/Контрагента, не позднее пяти рабочих дней, предоставить обновленную информацию Учреждению.

6.2 Учреждение обязано:

6.2.1. Обеспечить защиту и сохранность ПДн субъектов от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации.
6.2.2. Ознакомить субъекта ПДн с действующими внутренними правилами обработки ПДн.
6.2.3. Обеспечить защищенное хранение документов, содержащих ПДн. При этом ПДн не должны храниться дольше, чем этого требуют цели, для которых они были получены, или дольше, чем это требуется в интересах лиц, о которых собраны данные, или дольше, чем этого требует законодательство.
6.2.4. Организовать учет передачи ПДн Клиентов/Контрагентов третьим лицам путем ведения соответствующего Журнала учета передачи ПДн.
6.2.5. В случае реорганизации или ликвидации Учреждения, учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами и действующим законодательством Российской Федерации.
6.2.6. Организовать учет обращений субъектов ПДн в Журнале учета обращений субъектов ПДн.
6.2.7. Осуществлять передачу ПДн субъекта только в соответствии с законодательством Российской Федерации и настоящим Положением.
6.2.8. По требованию субъекта ПДн или его законного представителя предоставить ему полную информацию о его ПДн и обработке этих данных.
6.2.9. В случае отзыва Клиентом/Контрагентом согласия на обработку его персональных данных, и если сохранение персональных данных более не требуется для целей обработки персональных данных Учреждение обязано прекратить их обработку и обеспечить прекращение такой обработки другим лицом, действующим по поручению Учреждения, а также уничтожить персональные данные Клиента/Контрагента и обеспечить их уничтожение другим лицом, действующим по поручению Учреждения.
6.2.10. При обращении либо при получении запроса Клиента/Контрагента Учреждение в течение тридцати дней с даты получения запроса обязано сообщить Клиенту/Контрагенту информацию о наличии персональных данных о нем, и при необходимости предоставить возможность ознакомления с ними, либо в течение этого же срока дать мотивированный отказ в предоставлении информации.

## 7. 7. ПРАВА КЛИЕНТОВ И КОНТРАГЕНТОВ В ЦЕЛЯХ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Клиент и Контрагент имеет право:
7.1.1. На получение полной информации о составе своих ПДн и их обработке, в частности Клиент/Контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его ПДн.
7.1.2. На получение сведений об Учреждении, о месте его нахождения, о наличии в Учреждении персональных данных, относящихся к Клиенту/Контрагенту, а также на ознакомление с такими персональными данными.

7.1.3. Нас бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн Клиента/Контрагента на основании письменного запроса, за исключением случаев, если предоставление ПДн нарушает конституционные права и свободы других лиц и норм законодательства.
7.1.4. На выбор представителей для защиты своих ПДн.
7.1.5. На требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Учреждения персональных данных. При отказе Учреждения исключить или исправить ПДн Клиента/Контрагента, Клиент/Контрагент имеет право заявить в письменной форме Учреждению о своем несогласии с соответствующим обоснованием такого несогласия.
7.1.6. На требование об извещении Учреждением всех лиц, которым ранее были сообщены неверные или неполные ПДн Клиента/Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.
7.1.7. На обжалование в суде любых неправомерных действий или бездействия Учреждения при обработке и защите его ПДн.
7.2. Согласие на обработку персональных данных может быть отозвано Клиентом/Контрагентом.

## 8. 8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ПОЛУЧЕНИЕ, ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Каждый работник Учреждения, получающий для работы документ, содержащий персональные данные Клиента/Контрагента, несет персональную ответственность за сохранность носителя и конфиденциальность информации.
8.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут ответственность в соответствии с федеральными законами Российской Федерации и настоящим Положением.
8.3. Неправомерный отказ в предоставлении собранных в установленном порядке документов, содержащих персональные данные Клиентов/Контрагентов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации может повлечь наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

## 9. 9. ОБЕСПЕЧЕНИЕ НЕОГРАНИЧЕННОГО ДОСТУПА К НАСТОЯЩЕМУ ПОЛОЖЕНИЮ

9.1. Учреждение во исполнение требований п.2, ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» для обеспечения неограниченного доступа к сведениям о реализуемых Учреждением мероприятиях по защите персональных данных, и к документам, определяющим политику Учреждения в отношении обработки персональных данных, размещает текст настоящего

Положения на своем общедоступном сайте в глобальной телекоммуникационной сети Internet по адресу: https://zdorovie.clinic/.