УТВЕРЖДАЮ
Директор общества с ограниченной
ответственностью «Медлайн Барнаул»

_____ С.А. Ананина
«20» 07 2023 г.

ПОЛОЖЕНИЕ
о защите и обработке персональных данных сотрудников и пациентов общества с ограниченной ответственностью «Медлайн Барнаул»

1. Общие положения

1.1. Настоящее Положение о защите и обработке персональных данных сотрудников и пациентов (далее – Положение) разработано и применяется в обществе с ограниченной ответственностью «Медлайн Барнаул» в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Рекомендациями по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных, утвержденными Приказом Роскомнадзора от 19.08.2011 № 706, другими федеральными законами и нормативными актами, регулирующими вопросы защиты конфиденциальной информации.

1.2. Настоящее Положение определяет порядок получения, обработки, учёта, накопления, хранения и защиты от несанкционированного доступа и разглашения сведений, составляющих персональные данные сотрудников и пациентов общества с ограниченной ответственностью «Медлайн Барнаул» (далее – Медицинская организация), закрепление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Лицо, подписывающее трудовой договор с Медицинской организацией либо получающее платные медицинские услуги, автоматически соглашается с тем, что его персональные данные будут обрабатываться Медицинской организацией в соответствии с настоящим Положением. Сотрудник Медицинской организации не возражает против того, что некоторые его персональные данные согласно **Приложения № 1** станут общедоступными и доступ к ним не будет ограничен.

1.4. Настоящее Положение и изменения к нему утверждаются руководителем Медицинской организации по согласованию с лицом, ответственным за осуществление медицинской деятельности в Медицинской организации – главным врачом, вводятся в действие приказом Медицинской организации и подлежат опубликованию на сайте Медицинской организации. Все сотрудники Медицинской организации, работающие с персональными данными пациентов, должны быть ознакомлены с настоящим Положением под роспись.

2. Основные понятия

Для целей настоящего Положения используются следующие основные понятия:

- **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,

определенному или определяемому физическому лицу, пациенту, в том числе, его фамилия, имя, отчество, пол, год, месяц, дата и место рождения, адрес места жительства и регистрации, контактные телефоны, реквизиты полиса ОМС (ДМС), индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), паспортные данные, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью, данные о составе семьи, прочие сведения, которые могут идентифицировать человека.

- **персональные данные специальной категории** – персональные данные, касающиеся состояния здоровья. Персональные данные пациентов относятся к специальной категории персональных данных, обработка таких персональных данных должна осуществляться лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

Персональные данные пациентов являются конфиденциальными сведениями. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законодательством РФ.

Обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

- **субъект персональных данных** – лицо, обратившееся за медицинской помощью, независимо от наличия у него заболевания и состояния его здоровья (пациент), либо состоящее в трудовых отношениях с Медицинской организацией (сотрудник);
- **общедоступные персональные данные** – служебные персональные данные, доступ к которым неограничен и на которые не распространяется требование соблюдения конфиденциальности в связи с отсутствием негативных последствий для субъекта персональных данных в случае их раскрытия;
- **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;
- **неавтоматизированная обработка персональных данных** – обработка персональных данных без помощи 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;
- **конфиденциальность персональных данных** – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работника, требование не допускать их распространения без согласия субъекта персональных данных или

трудовой деятельности.

3. Состав и принципы обработки персональных данных

3.1. Обработка персональных данных субъектов персональных данных организуется и осуществляется Медицинской организацией на принципах:

- законности и справедливости;
- обработки только персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обеспечения точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

3.2. В состав персональных данных сотрудника, обрабатываемых Медицинской организацией, входит перечень документов, сопровождающий процесс оформления трудовых отношений с сотрудником в Медицинской организации при его приёме, назначении, переводе и увольнении, а также процесс оказания медицинских услуг гражданам.

3.3. Перечень персональных данных сотрудника, необходимый для оформления трудовых отношений, определяется Трудовым кодексом Российской Федерации.

3.4. Медицинская организация не имеет права получать и обрабатывать персональные данные сотрудников и пациентов, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, членства в общественных объединениях или профсоюзной деятельности.

3.5. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку в свободном волеизъявлении и в своем интересе. Согласие на обработку персональных данных даётся в письменной форме (**Приложение № 5 и № 6** к настоящему Положению) и должно быть конкретным, информированным и сознательным.

3.6. В случае необходимости проверки персональных данных пациента Медицинская организация должна заблаговременно сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствия отказа пациента дать письменное согласие на их получение.

3.7. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности сотрудника, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера заработной платы, установления медицинского диагноза и оказания пациенту медицинских услуг.

3.8. Обработка персональных данных ведется в неавтоматизированном и автоматизированном виде с учётом технологических процессов обработки персональных данных, в соответствии с внутренним приказом о допуске к обработке персональных данных, утверждённым руководителем Медицинской организации и обязательным для исполнения всеми сотрудниками.

3.9. Общедоступные персональные данные могут обрабатываться всеми структурными подразделениями Медицинской организации в автоматизированном и неавтоматизированном виде без установления требований по обеспечению безопасности информации. Обеспечение целостности указанных сведений осуществляется при необходимости.

3.10. Все персональные данные пациента следует получать у него самого. Персональные данные могут быть получены Медицинской организацией от лица, не являющегося субъектом

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». При наличии указанных оснований обработка персональных данных пациентов допускается без их согласия.

3.11. При недееспособности пациента согласие на обработку его персональных данных даёт его законный представитель.

3.12. В случае получения согласия на обработку персональных данных от представителя пациента полномочия данного представителя на дачу согласия от пациента проверяются Медицинской организацией.

3.13. Согласие пациента на обработку его персональных данных должно храниться вместе с его иной медицинской документацией.

3.14. Предоставление сведений о факте обращения пациента за оказанием медицинской помощи, сведений о состоянии его здоровья и диагнозе, иных сведений, полученных при его медицинском обследовании и лечении (врачебная тайна), без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения пациента, который в результате своего состояния не способен выразить свою волю, если медицинское вмешательство необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют его законные представители;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ», для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ».

3.15. Согласие на обработку персональных данных может быть отозвано пациентом (**Приложение № 7** к настоящему Положению). В случае отзыва пациентом согласия на обработку персональных данных Медицинская организация вправе продолжить обработку персональных данных без согласия пациента при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Обязанность предоставить доказательство получения согласия пациента на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», возлагается на Медицинскую организацию.

на обработку персональных данных. Образец согласия приведен в **Приложении № 4** к настоящему Положению.

3.17. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством.

3.18. В целях обеспечения прав и свобод человека и гражданина Медицинская организация и её представители при обработке персональных данных работников обязаны соблюдать следующие общие правила:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности сотрудника, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера заработной платы, предоставления гражданину медицинских услуг;
- обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- при определении объема и содержания, обрабатываемых персональных данных, Медицинская организация должна руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

4. Порядок получения Медицинской организацией персональных данных

4.1. Получение персональных данных Медицинской организацией может осуществляться как путем представления их самим субъектом персональных данных, так и путем получения их у третьей стороны на законных основаниях.

4.2. В целях обеспечения достоверности персональных данных сотрудник обязан предоставить в Медицинскую организацию комплекс достоверных, документированных персональных данных, состав которых установлен действующим законодательством РФ. Уполномоченное должностное лицо сверяет достоверность данных, представленных гражданином, с имеющимися у гражданина подлинными документами.

4.3. При заключении трудовых отношений либо договоров на платные услуги должно быть получено согласие сотрудника/пациента Медицинской организации на обработку его персональных данных. Образец согласия приведен в **Приложении № 5** к настоящему Положению.

4.4. В случае изменения персональных данных в процессе трудовых отношений сотрудник обязан письменно уведомить Медицинскую организацию о таких изменениях и предоставить изменившиеся данные в разумные сроки.

4.5. По мере необходимости, обусловленной спецификой выполняемых трудовых функций сотрудника, Медицинская организация вправе требовать от гражданина предоставления дополнительных сведений, содержащих персональные данные. Гражданин представляет необходимые сведения и в случае необходимости, предъявляет документы, подтверждающие достоверность этих данных.

4.6. Запрещается требовать от субъекта персональных данных предоставления персональных данных кроме предусмотренных Трудовым кодексом Российской Федерации, федеральными законами, указами Президента Российской Федерации, и т.п.

5. Хранение персональных данных

5.1. Персональные данные, обрабатываемые без использования средств автоматизации, представляют собой совокупность документов, сопровождающую процесс оформления трудовых отношений гражданина в Медицинской организации при его приеме, назначении, переводе и увольнении, а также пациента при получении им платных услуг.

5.2. Обязанность по ведению, хранению бумажных носителей, содержащих персональные данные, возлагается приказом руководителя Медицинской организации.

5.3. Персональные данные на бумажных носителях хранятся в закрывающихся на ключ

5.4. Перечень персональных данных, обрабатываемых в информационных системах, утверждается приказом руководителя Медицинской организации.

5.5. В отношении некоторых документов действующим законодательством Российской Федерации могут быть установлены иные требования хранения, чем предусмотрено настоящим Положением. В таких случаях следует руководствоваться правилами, установленными соответствующим нормативным актом.

6. Передача персональных данных

6.1. Передача персональных данных третьей стороне должна осуществляться только при условии обязательного выполнения требования конфиденциальности.

6.2. От лица, чьи персональные данные передаются третьей стороне, должно быть получено согласие на передачу этих данных.

6.3. При передаче персональных данных работники Медицинской организации, имеющие доступ к персональным данным, должны осуществлять передачу в соответствии с настоящим Положением и действующим законодательством Российской Федерации.

6.4. Персональные данные не должны быть переданы третьей стороне без письменного согласия субъекта персональных данных, за исключением следующих случаев:

- осуществляется передача общедоступных персональных данных;
- передача персональных данных осуществляется при условии обязательного обезличивания персональных данных;
- передача персональных данных является требованием действующего федерального законодательства;
- передача персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов гражданина, если получение его согласия невозможно, а также передача персональных данных необходима для прохождения медицинской комиссии сотрудника.

6.5. Учитывая, что Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта персональных данных, Медицинская организация в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных гражданина, либо отсутствует его письменное согласие на предоставление персональных сведений, либо, по мнению Медицинской организации, отсутствует угроза жизни или здоровью субъекта персональных данных, Медицинская организация обязана отказать в предоставлении персональных данных лицу.

6.6. При передаче персональных данных третьей стороне должны быть переданы только те данные, которые необходимы третьей стороне для достижения целей обработки, а также на которые было получено согласие субъекта персональных данных. Образец согласия приведен в **Приложении № 3** к настоящему Положению.

6.7. Решение о передаче персональных данных третьей стороне рассматривается руководителем структурного подразделения, от которого требуются эти данные. При принятии решения ему необходимо руководствоваться законодательством Российской Федерации и настоящим Положением. В случае если законность передачи персональных данных третьей стороне вызывает сомнения, руководитель структурного подразделения обращается к ответственному за обработку персональных данных для получения необходимых разъяснений. Окончательное решение о возможности передачи персональных данных третьей стороне принимается руководителем Медицинской организации.

6.8. Медицинская организация не должна сообщать персональные данные третьей стороне в коммерческих целях без письменного согласия субъекта персональных данных.

6.9. Лицо, получившее персональные данные от Медицинской организации, должно быть предупреждено, что эти данные могут быть использованы лишь в целях, для которых они были переданы.

6.10. Доступ к персональным данным, обрабатываемых в Медицинской организации, может быть предоставлен только специально уполномоченным лицам, при этом указанные лица должны

иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

6.11. Медицинская организация может осуществлять передачу персональных данных в электронном виде по каналам связи в соответствии с действующим законодательством РФ, с условием соблюдения необходимых мер информационной безопасности.

7. Обеспечение безопасности персональных данных

7.1. Персональные данные относятся к конфиденциальной информации.

7.2. Перечень должностных лиц, имеющих доступ к обработке персональных данных и прочих конфиденциальных данных, утверждается приказом руководителя Медицинской организации.

7.3. Для сотрудника Медицинской организации, получившего доступ к персональным данным, обязательным является требование не допускать распространение данной информации без согласия субъекта персональных данных, а также без иного законного основания. Перед получением доступа к персональным данным сотрудник Медицинской организации подписывает обязательство о неразглашении информации, содержащей персональные данные, согласно **Приложению № 2** настоящего Положению.

7.4. Сотрудники Медицинской организации, получившие доступ к персональным данным, для соблюдения режима конфиденциальности должны руководствоваться требованиями настоящего Положения, должностных регламентов, а также локальных организационно-распорядительных документов Медицинской организации.

7.5. Обо всех фактах и попытках нарушения безопасности персональных данных сотрудники Медицинской организации обязаны ставить в известность ответственных за обработку персональных данных, а также руководителя Медицинской организации.

7.6. При передаче персональных данных третьей стороне должен использоваться безопасный канал передачи. Запрещается передавать персональные данные (кроме общедоступных) через сеть международного информационного обмена (отправлять по электронной почте и т.п.) без применения необходимых программных и/или аппаратных средств защиты. За организацию безопасного канала передачи персональных данных третьей стороне отвечает администратор безопасности информации.

7.7. Ответственные за обработку персональных данных контролируют соблюдение требований федеральных законов по защите персональных данных и организуют мероприятия по их реализации. Администратор безопасности информации обеспечивает техническое обслуживание и сопровождение средств защиты персональных данных.

7.8. Электронные носители информации, содержащие персональные данные, учитываются администратором безопасности информации в соответствующем журнале.

7.9. Съемные электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах. При этом необходимо создать надлежащие условия, обеспечивающие их сохранность. Правила работы со съемными носителями, содержащими персональные данные, закреплены локальными организационно-распорядительными документами, за разработку которых отвечает администратор безопасности информации.

7.10. Защита персональных данных от неправомерного их использования или утраты обеспечивается Медицинской организацией за счет собственных средств в порядке, установленном действующим законодательством РФ.

8. Права гражданина в целях защиты персональных данных

8.1. В целях обеспечения защиты персональных данных, обрабатываемых Медицинской организацией, субъект персональных данных имеет право на:

8.1.2. Свободный бесплатный доступ ко всем своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральными законами.

8.1.3. Определение своих представителей для защиты своих персональных данных.

8.1.4. Ознакомление с отзывами о своей профессиональной служебной деятельности и другими документами до внесения их в личное дело, материалами личного дела, а также на приобщение к личному делу письменных объяснений и других документов и материалов.

8.1.5. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований федерального закона. При отказе Медицинской организации исключить или исправить персональные данные гражданина, он имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием своей позиции. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения.

8.1.6. Обжалование в суд любых неправомерных действий или бездействия Медицинской организации при обработке и защите его персональных данных.

8.2. Доступ к своим персональным данным предоставляется должностному лицу или его законному представителю Медицинской организацией при обращении либо при получении письменного запроса субъекта персональных данных или его законного представителя. Запрос должен содержать данные основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта или его законного представителя. Обращения субъектов персональных данных фиксируются в журнале учета обращений субъектов персональных данных.

9. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных

9.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

9.2. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.3. Руководитель Медицинской организации, разрешая передачу персональных данных третьей стороне, несет персональную ответственность за данное разрешение в соответствии с действующим законодательством Российской Федерации.