Индивидуальный предприниматель
Матюшечкин Игорь Викторович
(Глазная клиника доктора Матюшечкина И.В.)

ПРИКАЗ № 200201

г. Петрозаводск «20» февраля 2025 года

Об утверждении положения об обработке и защите персональных данных

В соответствии с Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», постановлением Правительства Российской Федерации от 12.11.2012 г. №1152 «Об утверждении положения о государственном контроле качества и безопасности медицинской деятельности», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях обеспечения внутреннего контроля качества и безопасности медицинской деятельности у ИП Матюшечкина И.В.

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке и защите персональных данных (Приложение № 1).
2. Контроль за исполнением настоящего приказа оставляю за собой.

Индивидуальный предприниматель		Матюшечкин И.В.
(должность)	(личная подпись)	(расшифровка подписи)

Приложение 1

к приказу от 20 февраля 2025 года № 200201

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ГЛАЗНОЙ КЛИНИКЕ ДОКТОРА МАТЮШЕЧКИНА И.В.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан», другими федеральными законами и нормативными актами, регулирующими вопросы защиты конфиденциальной информации.

1.2. Цель разработки Положения – определение порядка обработки и защиты персональных данных в Глазной клинике доктора Матюшечкина И.В. (далее - Клиника), 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 Клиникой/получающее платные услуги, автоматически соглашается с тем, что его персональные данные будут обрабатываться Клиникой в соответствии с настоящим Положением. Работник Клиники, в том числе, признает тот факт, что он не возражает против того, что некоторые данные (указанные в Приложении 1) станут общедоступными и доступ к ним не будет ограничен.

1.4. Цель обработки персональных данных - заключение договора с физическими лицами на оказание платных медицинских услуг; осуществление трудовых взаимоотношений с работниками.

1.5. Категории и перечни обрабатываемых персональных данных - непосредственно персональные данные: фамилия, имя, отчество; год, месяц, дата и место рождения, адрес, паспортные данные, номер телефона, образование, профессия, доходы, данные трудовой книжки, данные военного билета, сведения о пенсионном страховании, ИНН, семейное положение.

1.6. Категории субъектов, персональные данные которых обрабатываются: лица, заключающие договор на оказание платных медицинских услуг (пациенты), заказчики и законные представители несовершеннолетних пациентов; работники, состоящие в трудовых отношениях с ИП Матюшечкиным И.В.

1.7. Способ обработки персональных данных - смешанная обработка персональных данных (и автоматизированный, и неавтоматизированный способы одновременно).

Дата начала обработки персональных данных – 17 июля 2018 года.

Прекращение обработки персональных данных происходит в случае прекращения деятельности ИП Матюшечкина И.В., истечения срока хранения, предусмотренного законом, договором или согласием субъекта персональных данных на обработку его персональных данных, отзыва субъектом персональных данных (или его представителем) согласия на обработку его персональных данных с учетом достижения условий, предусмотренных ст. 21 ФЗ «О персональных данных».

2. Основные понятия

Для целей настоящего Положения используются следующие основные понятия:

2.1. **Работник Клиники** – лицо, вступившее в трудовые отношения с Клиникой (далее – должностное лицо, работник, сотрудник);

2.2. **Персональные данные** – любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (субъект персональных данных, гражданин), необходимая Клинике в связи с трудовыми отношениями при оказании платных услуг;

2.3. **Персональные данные специальной категории** – персональные данные, касающиеся состояния здоровья;

2.4. **Общедоступные персональные данные** – служебные персональные данные, доступ к которым не ограничен и на которые не распространяется требование соблюдения конфиденциальности в связи с отсутствием негативных последствий для субъекта персональных данных в случае их раскрытия;

2.5. **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,

2.6. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

2.7. **Неавтоматизированная обработка персональных данных** – обработка персональных данных без помощи средств вычислительной техники;

2.8. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.9. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

2.10. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.11. **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;

2.12. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

2.13. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

2.14. **Конфиденциальность персональных данных** – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работника, требование не допускать их распространения без согласия работника или иного законного основания;

2.15. **Личное дело** – совокупность документов, содержащих сведения о должностном лице и его трудовой деятельности.

3. Состав и принципы обработки персональных данных

3.1. В состав персональных данных, обрабатываемых Клиникой, входит комплекс документов, сопровождающий процесс оформления трудовых отношений с работником в Клинике при его приеме, назначении, переводе и увольнении, а также процесс оказания медицинских услуг гражданам.

3.2. Клиника не имеет право получать и обрабатывать персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, членства в общественных объединениях или его профсоюзной деятельности.

3.3. Перечень персональных данных работника, необходимый для оформления трудовых отношений, определяется Трудовым Кодексом Российской Федерации;

3.4. Персональные данные граждан обрабатываются Клиникой в соответствии со ст. 43, 44 Федерального закона от 29.11.2010 года №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

3.5. Клиникой определен перечень сведений конфиденциального характера, согласно которому происходит обработка следующих категорий персональных данных:

- персональные данные работников Клиники;
- персональные данные получателей платных услуг Клиники;

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

3.7. Обработка персональных данных ведется в неавтоматизированном и автоматизированном виде в соответствие со следующими локальными нормативными актами:

- Перечень информационных систем, обрабатывающих персональные данные;
- Приказы о допуске к обработке персональных данных;
- Технологические процессы обработки персональных данных.

Указанные локальные нормативные акты утверждаются руководителем Клиники и обязательны для исполнения всеми сотрудниками.

3.8. Для публикации (размещения в общедоступном источнике) персональных данных, помимо отнесенных к общедоступным, необходимо получение согласия субъекта на обработку персональных данных. Образец согласия приведен в Приложении 4 к настоящему Положению.

3.9. 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.

3.10. В целях обеспечения прав и свобод человека и гражданина Клиника и ее представители при обработке персональных данных работников обязаны соблюдать следующие общие правила:

3.10.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности работника, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера заработной платы, предоставления гражданину медицинских услуг;

3.10.2. Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

3.10.3. При определении объема и содержания обрабатываемых персональных данных Клиника должна руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

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

3.10.5. Защита персональных данных от неправомерного их использования или утраты обеспечивается Клиникой за счет собственных средств в порядке, установленном федеральными законами.

4. Порядок получения Учреждением персональных данных

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

4.2. При заключении трудовых отношений либо договоров на платные услуги должно быть получено согласие работника/пациента Клиники на обработку его персональных данных. Образец согласия приведен в Приложении 5 к настоящему Положению.

4.3. В случае изменения персональных данных в процессе трудовых отношений гражданин обязан письменно уведомить Клинику о таких изменениях и предоставить изменившиеся данные в разумные сроки.

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

4.5. 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 Клинике при его приеме, назначении, переводе и увольнении, а также гражданина при получении им платных услуг.

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

5.3. Перечень персональных данных, обрабатываемых в информационных системах, утверждается приказом руководителя Клиники.

5.4. 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 Клиники, 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 закона или договора между субъектом и Клиникой;
- 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 работника.

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, Клиника 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 Клиники, отсутствует угроза жизни или здоровью субъекта персональных данных, Клиника обязана отказать в предоставлении персональных данных лицу.

6.5. 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.

6.6. Решение о передаче персональных данных третьей стороне принимается руководителем Клиники. При принятии решения ему необходимо руководствоваться законодательством Российской Федерации и настоящим Положением. В случае если законность передачи персональных данных третьей стороне вызывает сомнения, руководитель Клиники обращается к ответственному за обработку персональных данных для получения необходимых разъяснений.

6.7. Клиника не должна сообщать персональные данные третьей стороне в коммерческих целях без письменного согласия субъекта персональных данных.

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

6.9. Доступ к персональным данным, обрабатываемых в Клинике, 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.

6.10. Клиника может осуществлять передачу персональных данных в электронном виде по каналам связи в соответствие с Законодательством РФ, а также регламентами, указанными в п. 4.1, 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 директора.

7.3. Для сотрудника Клиники, 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 работник Клиники подписывает обязательство о неразглашении информации, содержащей персональные данные, согласно Приложению 2 настоящего Положению.

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

7.5. Обо всех фактах и попытках нарушения безопасности персональных данных работники Клиники обязаны ставить в известность ответственных за обработку персональных данных руководителя Клиники.

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 руководитель Клиники.

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

8. Права гражданина в целях защиты персональных данных

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

8.1.1. 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;

8.1.2. Определение своих представителей для защиты своих персональных данных;

8.1.3. 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;

8.1.4. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований федерального закона. При отказе Клиники 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;

8.1.5. Обжалование в суд любых неправомерных действий или бездействия Клиники при обработке и защите его персональных данных.

8.1.6. Доступ к своим персональным данным предоставляется должностному лицу или его законному представителю Клиникой при обращении либо при получении письменного запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта 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. Руководитель Клиники, разрешая передачу персональных данных третьей стороне, несет персональную ответственность за данное разрешение в соответствии с законодательством Российской Федерации.

10. Порядок уничтожения персональных данных

10.1. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть максимально надежным и конфиденциальным, исключая возможность последующего восстановления;
- оформляться юридически, в частности, актом о выделении носителей, содержащих персональные, к уничтожению и актом об уничтожении носителей, содержащих персональные данные;
- должно проводиться комиссией по уничтожению персональных данных;
- уничтожение должно касаться только тех носителей, содержащих персональные данные, которые подлежат уничтожению в связи с достижением цели обработки указанных персональных данных либо утраты необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

10.2. Персональные данные хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, но не ранее истечения срока для хранения данных установленных действующим законодательством.

Носители, содержащие персональные данные, уничтожаются комиссией по уничтожению персональных данных, утвержденной приказом руководителя Организации (далее - Комиссия).

Носители, содержащие персональные данные, уничтожаются Комиссией в срок, не превышающий тридцати дней с даты, указанной в абзаце первом пункта 10.2 настоящего положения.

Комиссия производит отбор бумажных и машиночитаемых носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

На все отобранные к уничтожению носители составляется акт.

В акте на уничтожение носителей исправления не допускаются.

Комиссия проверяет наличие всех носителей, включенных в акт.

По окончании сверки акт подписывается всеми членами комиссии и утверждается руководителем Организации.

Носители, содержащие персональные данные, отобранные для уничтожения и включенные в акт, после проверки их Комиссией складываются и опечатываются председателем комиссии.

Уничтожение носителей, содержащих персональные данные, производится после утверждения акта в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных

данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уничтожение носителей, содержащих персональные данные, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем сжигания или измельчения на мелкие части, исключающие возможность последующего восстановления информации;
- уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных.

Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя или его сжигания;

- подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске, удаляются средствами операционной системы компьютера с последующим "очищением корзины";
- в случае допустимости повторного использования носителя FDD, CD-RW, DVD-RW применяется программное удаление ("затирание") содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

10.3. Об уничтожении носителей Комиссия составляет и подписывает акт об уничтожении, который направляется на утверждение руководителю Организации

В акте указываются:

- дата, место и время уничтожения;
- должности, фамилии, инициалы членов комиссии;
- вид и количество уничтожаемых носителей, содержащих персональные данные;
- основание для уничтожения;
- способ уничтожения.

Факт уничтожения носителей, содержащих персональные данные, фиксируется в акте. Данный документ является документом конфиденциального характера и вместе с актами уничтожения хранится в документации организации