УТВЕРЖДАЮ
Генеральный директор
ООО «Центр диагностики Ногинск»
_____Е.В. Весновская
01 марта 2023г.

Положение
о работе с персональными данными пациентов
ООО «Центр диагностики Ногинск»

1. Общие положения

1.1. Настоящим Положением определяется порядок сбора, систематизации, накопления, уточнения, использования, хранения, распространения и защиты персональных данных клиентов ООО «Центр диагностики Ногинск» (далее - Клиника).

1.2. Настоящее Положение разработано в строгом соответствии с требованиями:
– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
– Федерального закона от 21.07.2014 № 242 «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;
– Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
– постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
– постановления Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
– приказа ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящее Положение разработано с учетом понимания законодательства о персональных данных, изложенного в Научно-практическом комментарии к Федеральному закону «О персональных данных» под ред. зам. руководителя Федеральной службы Роскомнадзора Приезжевой А.А.

2. Персональные данные клиентов (пациентов)

2.1. Состав сведений (персональных данных) о клиентах и цели их обработки:

2.1.1. Персональные данные пациентов (лиц, являющихся стороной договора на оказание медицинских услуг), обрабатываемые в клинике:
– паспортные данные;
– номера телефонов для связи с пациентом (контактная информация);
– информация о состоянии здоровья пациента, поставленных диагнозах, проведенном или планируемом к проведению медицинском вмешательстве.

2.1.2. Персональные данные пациентов, полученные при заключении договора на медицинские услуги, обрабатываются только в целях предоставления качественной медицинской помощи, проведения оценки качества оказываемых услуг, в целях обеспечения оплаты лечения пациентов посредством страховых компаний.

2.1.3. Клиника обеспечивает конфиденциальность персональных данных клиентов и обязана не допускать их распространения без согласия клиентов либо наличия иного законного основания.

2.1.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиентов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

2.2. Порядок обработки персональных данных клиентов:

2.2.1. Предприятие получает персональные данные непосредственно от субъекта персональных данных – клиента на основании заключения с клиентом письменного договора на оказание медицинских услуг.

2.2.2. В силу подпункта 5 части 1 статьи 6, подпункта 4 части 2 статьи 10 Федерального закона от 27.07.2006 № 152-ФЗ письменного согласия на обработку персональных данных о здоровье пациента не требуется.

По смыслу части 1 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ рентгеновские снимки, СД-диск с изображением исследований, заключения пациентов не являются биометрическими данными, поскольку не используются оператором для установления личности субъекта персональных данных.

Согласие на обработку персональных данных пациентов берется клиникой с целью демонстрации пациентам серьезности намерений соблюдения конфиденциальности, а также с целью предупреждения о тех случаях, когда информация о здоровье пациента может быть передана третьим лицам без его согласия.

2.2.3. Персональные данные клиента обрабатываются клиникой исключительно для достижения целей, определенных письменным договором между клиентом и клиникой, в частности, для оказания медицинских услуг клиенту.

2.2.4. Обработка персональных данных клиентов ведется методом смешанной (в том числе автоматизированной) обработки.

2.2.5. К обработке персональных данных клиента могут иметь доступ только сотрудники клиники, допущенные к работе с персональными данными клиента.

2.2.6. Отзыв пациентом согласия на обработку персональных данных о здоровье не влечет прекращения обработки персональных данных в силу части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ.

2.2.7. Клиника уничтожает персональные данные клиента, за исключением данных, содержащихся в медицинской карте и иной медицинской документации, в следующие сроки: хранящиеся на электронных носителях – в течение трех рабочих дней с момента расторжения договора или отзыва согласия на обработку.

2.2.8. Передачу персональных данных клиента клиника производит исключительно для достижения целей, определенных письменными договорами между клиентом и клиникой, в частности, для оплаты медицинских услуг, оказываемых на основании договоров добровольного медицинского страхования.

Надлежаще заверенную копию медицинской карты пациента для экспертизы страховой компании клиника передает в бумажном виде. Передача копии по запросу страховой компании в силу подпункта 8 части 2 статьи 10 Федерального закона от 27.07.2006 № 152-ФЗ не требует письменного согласия пациента.

2.2.9. Без согласия клиента персональные данные о состоянии его здоровья могут быть переданы в случаях, прямо предусмотренных статьей 13 Федерального закона от 21.11.2011 № 323-ФЗ, в случае возникновения угрозы распространения инфекционных заболеваний (гепатиты, ВИЧ, сифилис, ОРИ, туберкулез), о чем клиент уведомляется в согласии на обработку его персональных данных.

2.2.10. Персональные данные клиентов содержатся в следующих группах документов:

– договор на оказание медицинских услуг и все приложения к нему;

– согласие родителей на подписание договора несовершеннолетним;

– анкета о здоровье;

– медицинская карта;

– информированные согласия на различные виды медицинских манипуляций;

– протоколы фиксации претензий пациента.

2.2.11. Персональные данные клиентов могут храниться как на бумажных носителях, так и в электронном виде.

2.2.12. Персональные данные клиентов на бумажных носителях, если с них не снят на законном основании режим конфиденциальности, хранятся в специально отведенных железных шкафах. Ключи от железных шкафов хранятся лично у медицинского регистратора, допущенной к обработке персональных данных клиентов.

2.2.13. Персональные данные клиентов также хранятся в электронном виде – в локальной компьютерной сети клиники, в базах данных, каталогах и файлах, размещенных на серверах клиники, доступ к которым разрешен сотрудникам, допущенным к обработке персональных данных клиентов.

2.2.14. При передаче персональных данных клиента клиника должна соблюдать следующие требования:

– не сообщать персональные данные клиента третьей стороне без письменного согласия клиента, за исключением случаев, установленных федеральным законом;

– не сообщать персональные данные клиента в коммерческих целях без его письменного согласия;

– предупредить лиц, получающих персональные данные клиента о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

– разрешать доступ к персональным данным клиентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные клиентов, которые необходимы для выполнения конкретных функций.

2.3. Права и обязанности клиники при обработке персональных данных клиента (пациента):

2.3.1. В целях обеспечения прав и свобод человека и гражданина клиника и ее сотрудники при обработке персональных данных клиента обязаны соблюдать следующие общие требования:

– при определении объема и содержания персональных данных клиента, подлежащих обработке, руководствоваться федеральными законами от 27.07.2006 № 152-ФЗ и от 21.11.2011 № 323-ФЗ, а также договорными обязательствами, взятыми на себя сторонами по договору между клиентом и клиникой;

– не получать и не обрабатывать персональные данные клиента о его судимости, политических, религиозных и иных убеждениях и частной жизни.

2.3.2. Клиника должна обеспечить защиту персональных данных клиента от неправомерного их использования или утраты за собственный счет в порядке, установленном федеральным законодательством.

2.3.3. Клиника обязана сообщить клиенту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомиться с ними:

– в течение трех рабочих дней с момента обращения (подачи запроса), если речь идет о предоставлении медицинской справки или медицинского заключения;

– пяти рабочих дней с момента обращения (подачи запроса), если речь идет о предоставлении информации в виде копии медицинской карты.

2.3.4. Все сотрудники, связанные с получением, обработкой и защитой персональных данных клиентов, обязаны подписать уведомление-обязательство о неразглашении персональных данных клиентов (Приложение 1).

Процедура оформления доступа к персональным данным клиента включает:

– ознакомление сотрудника под подпись с настоящим Положением. При наличии иных нормативных актов (приказов, распоряжений, инструкций), регулирующих обработку и защиту персональных данных клиента, с данными актами также производится ознакомление под подпись;

– уведомление сотрудника о факте обработки персональных данных;

– истребование с сотрудника (за исключением директора) письменного обязательства о соблюдении конфиденциальности персональных данных клиентов и соблюдении правил их обработки. Обязательство готовят по установленной форме (приложение 1).

2.3.5. Сотрудник клиники, имеющий доступ к персональным данным клиентов в связи с исполнением трудовых обязанностей:

– обеспечивает хранение информации, содержащей персональные данные клиента, исключающее доступ к ним третьих лиц;

– не оставляет на рабочем месте документы, содержащие персональные данные клиентов;

– при уходе в отпуск, во время служебной командировки и в иных случаях длительного отсутствия передает документы и иные носители, содержащие персональные данные клиентов, директору клиники.

2.3.6. Допуск к персональным данным клиента других сотрудников клиники, не имеющих надлежащим образом оформленного доступа, запрещается.

2.4. Права и обязанности клиента (пациента)

2.4.1. Клиент обязан передавать клинике или ее представителю комплекс достоверных, документированных персональных данных, состав которых установлен настоящим Положением и договорными обязательствами, взятыми на себя сторонами по договору между клиентом и клиникой.

2.4.2. Клиент должен без неоправданной задержки сообщать клинике об изменении своих персональных данных.

2.4.3. Клиент имеет право на получение сведений о клинике, о ее местонахождении, о наличии у клиники персональных данных, относящихся к клиенту, а также на ознакомление с такими персональными данными.

Клиент вправе требовать от клиники уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2.4.4. Доступ клиента к своим персональным данным предоставляется на основании письменного запроса пациента на имя главного врача клиники. Запрос должен содержать номер основного документа, удостоверяющего личность клиента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись клиента или его законного представителя.

2.4.5. Сведения о наличии персональных данных должны быть предоставлены клиенту в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

2.4.6. Клиент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных клиникой, а также цель такой обработки;

– способы обработки персональных данных, применяемые клиникой;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для клиента может повлечь обработка его персональных данных.

2.4.7. Клиент имеет право отозвать согласие на обработку персональных данных, ограничить способы и формы обработки персональных данных, запретить

распространение персональных данных без его согласия. Отзыв пациентом согласия на обработку персональных данных о здоровье не влечет прекращения обработки персональных данных в силу части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ.

2.4.8. Клиент вправе обжаловать действия или бездействие клиники в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.4.9. Клиент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

3. Система мер защиты персональных данных

3.1. Общую организацию защиты персональных данных клиентов осуществляет директор клиники.

3.2. Защиту персональных данных, хранящихся в электронных базах данных клиники, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий обеспечивает специалист IT, находящийся в штате предприятия либо оказывающий услуги на основании договора подряда.

3.3. Система мер защиты персональных данных в зависимости от типа угроз включает в себя:

Наименование угрозы	Меры по противодействию угрозе	
	Технические	Организационные
1. конкуренты конкретной компании, желающие нанести ей ущерб	избежать неправомерного доступа к данным как со стороны внешних посягателей, так и со стороны инсайдеров.	разработка соглашений с третьими лицами, согласно которым им поручается обработка данных с внедрением в них мер ответственности и норм о возмещении возможного ущерба;
2. международные кибертеррористические организации, заинтересованные в утечках персональных данных в целях обеспечения собственного пиара	предотвратить утечку данных по техническим каналам	определение актуальной модели угроз с учетом анализа внешних и внутренних факторов;
3. инсайдеры, сотрудники компании, руководствующиеся своими целями или действующие по чужим поручениям.		ранжирование лиц, имеющих разные степени допуска к конфиденциальным данным, подписание с ними соглашений о соблюдении коммерческой тайны;

Помимо организационно-технических мер клиника принимает правовые меры для защиты персональных данных, а именно издает локальные правовые акты, направленные на регулирование обработки персональных данных в рамках клиники:

– Положение об обработке персональных данных в организации;

– Политика в отношении обработки персональных данных в организации;
– приказ о назначении ответственного за обработку персональных данных;
– приказ об утверждении перечня обрабатываемых персональных данных;
– приказ о допуске сотрудников к обработке персональных данных;
– приказ об обработке персональных данных без использования средств автоматизации;
– приказ о разработке комплекса организационно-технических мер по защите персональных данных с использованием средств автоматизации;
– приказ о форме запросов субъектов персональных данных;
– приказ о компенсационных мерах по защите персональных данных и др.

4. Ответственность за разглашение персональных данных

4.1. Клиника несет ответственность за разработку, введение и действенность соответствующих требованиям законодательства норм, регламентирующих получение, обработку и защиту персональных данных клиента и сотрудников. Клиника закрепляет персональную ответственность сотрудников за соблюдение установленного в организации режима конфиденциальности.

4.2. Руководитель, разрешающий доступ сотрудника к документам, содержащим персональные данные клиента, несет персональную ответственность за данное разрешение.

4.3. Каждый сотрудник клиники, получающий для работы документ, содержащий персональные данные клиента, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

4.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных клиента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами:

– статьи 150, 151 Гражданского кодекса – гражданско-правовая ответственность;
– статья 13.14 КоАП – административная ответственность;
– статья 137 Уголовного кодекса – уголовная ответственность.

4.5. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных клиентов клиника вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания, в том числе увольнение на основании подпункта «в» пункта 6 статьи 81 Трудового кодекса за разглашение персональных данных другого работника.

5. Заключительные положения

Настоящее Положение вступает в силу с момента издания приказа директора организации о введении Положения в силу и обязательно для ознакомления, соблюдения и исполнения всеми сотрудниками организации.

Лист ознакомления
с локальным нормативным актом

№ п/п	Фамилия, имя, отчество	Наименование должности	Дата ознакомления с Положением об обработке ПД	Подпись работника
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Приложение 1
к Положению об обработке
персональных данных (ПД)
в ООО «Центр диагностики Ногинск»

Уведомление-обязательство
сотрудников ООО «Центр диагностики Ногинск» при работе с персональными данными

Настоящим я уведомлен, что, являясь сотрудником ООО «Центр диагностики Ногинск», осуществляю сбор, обработку, дополнение и хранение персональных данных (пациентов).

Обязуюсь осуществлять сбор, обработку, хранение, а также в предусмотренных законом случаях передачу персональных данных:
– только в объемах, необходимых для исполнения моих трудовых обязанностей;
– только в соответствии с правилами, ограничениями и запретами, предусмотренными в настоящем Положении.

Обязуюсь не разглашать персональные данные пациентов, ставшие мне известными в процессе исполнения трудовых обязанностей.

Ф. И. О.	Должность	Категория персональных данных, к которой имеется доступ