Приложение к приказу
АНО «Центр профессиональной
патологии и лабораторной диагностики»
от «02» сентября 2019 г. № 39

ПОЛОЖЕНИЕ
об обработке персональных данных
в АНО «Центр профессиональной патологии
и лабораторной диагностики»

1. Общие положения

1.1. Настоящее Положение имеет своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Настоящее Положение об обработке персональных данных (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных (далее – ПДн).

1.3. 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», Постановления Правительства РФ №1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Федерального закона от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», иными нормативно-правовыми актами, действующими на территории Российской Федерации.

2. Информация об операторе

Наименование: Автономная некоммерческая организация «Центр профессиональной патологии и лабораторной диагностики».

ИНН: 8601065060.

Фактический адрес: 628010, Российская Федерация, г. Ханты-Мансийск, ул. Тобольский тракт, д. 4.

Телефон: + 7(3467) 35-10-20.

3. Основные понятия

Для целей настоящего Положения используются следующие понятия:

3.1. Оператор ПДн (далее Оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПДн, а также определяющие цели и содержание обработки ПДн.

3.2. ПДн - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу.

3.3. Субъект - субъект ПДн.

3.4. Обработка ПДн - любое действие (операция) или совокупность действий (операций) с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3.5. Распространение ПДн - действия, направленные на передачу ПДн определенному кругу лиц или на ознакомление с ПДн неограниченного круга лиц, в том числе опубликование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

3.6. Блокирование ПДн - временное прекращение сбора, систематизации, накопления, использования, распространения ПДн, в том числе их передачи.

3.7. Уничтожение ПДн - действия, в результате которых невозможно восстановить содержание ПДн в информационной системе персональных данных (далее – ИСПДн) или в результате которых уничтожаются материальные носители персональных данных.

3.8. Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

4. Категории субъектов персональных данных

4.1. Работник Оператора – субъект ПДн, состоящий с Оператором в трудовых отношениях.

4.2. Пациент – субъект ПДн, получающий медицинские и/или лабораторные услуги, оказываемые Оператором.

4.3. Гость – субъект ПДн, имеющий намерение заказать или приобрести либо заказывающий, приобретающий и/или использующий гостиничные услуги исключительно для личных и иных нужд, не связанных с осуществлением предпринимательской деятельности.

5. Состав персональных данных

5.1. Состав ПДн работников Оператора: фамилия, имя, отчество; дата рождения; место рождения; адрес проживания; адрес прописки; семейное положение; социальное положение; имущественное положение; сведения об образовании; сведения о профессии; сведения о доходах; сведения о состоянии здоровья; фотографии; пол; гражданство; реквизиты документа, удостоверяющего личность; номер телефона; адрес электронной почты; сведения о постановке на учет в налоговом органе; реквизиты полиса ОМС (ДМС); страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС); сведения о воинском учете; сведения о социальных льготах; должность; сведения о трудовой деятельности; сведения о повышении квалификации, переподготовке и аттестации; сведения о судимости; место работы или учебы членов семьи; содержание служебного контракта; содержание приказов по личному составу; основания к приказам по личному составу; сведения о награждении государственными наградами, присвоении почетных, воинских и специальных званий.

5.2. Состав ПДн пациентов: фамилия, имя, отчество; дата рождения; место рождения; пол; адрес проживания; адрес прописки; контактный телефон; адрес электронной почты; реквизиты документа, удостоверяющего личность; реквизиты полиса ОМС (ДМС); сведения о месте работы или учёбы; страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС); сведения о выписанных

лекарственных средствах; данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью.

5.3. Состав ПДн гостей: фамилия, имя, отчество; дата рождения; место рождения; пол; адрес проживания; адрес прописки; контактный телефон; адрес электронной почты; реквизиты документа, удостоверяющего личность.

6. Цели обработки персональных данных

6.1. Цели обработки ПДн работников Оператора:

- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений;
- ведение кадрового и бухгалтерского учёта работников Оператора.

6.2. Цели обработки ПДн пациентов:

- организация и оказание медицинской помощи;
- проведение медицинских осмотров;
- проведение медицинских освидетельствований;
- проведение медицинских экспертиз.

6.3. Цели обработки ПДн гостей:

- исполнение договора оказания гостиничных услуг;
- предоставление дополнительных услуг.

7. Меры по обеспечению безопасности персональных данных

7.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

7.2. Обработка ПДн может осуществляться исключительно в целях, указанных в настоящем Положении.

7.3. Обработка и хранение ПДн, обрабатываемых для различных целей, осуществляется раздельно.

7.4. Основными мерами защиты ПДн Оператором являются:

7.4.1. назначение лица, ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением Оператором и его работниками требований к защите ПДн;

7.4.2. определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;

7.4.3. разработка положения в отношении обработки персональных данных;

7.4.4. контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности информационных систем;

7.4.5. установление правил доступа к ПДн, обрабатываемых в ИСПДн, обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн, а так же обнаружение фактов несанкционированного доступа к ПДн и принятие мер;

7.4.6. своевременное обнаружение фактов несанкционированного доступа к ПДн;

7.4.7. возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7.4.8. использование сертифицированных программных и аппаратных средств защиты ПДн.

8. Права и обязанности субъектов ПДн и Оператора

8.1. Работники Оператора, непосредственно осуществляющие обработку ПДн, должны быть ознакомлены с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами в отношении обработки ПДн, Положением об обработке ПДн.

8.2. Перечень лиц, имеющих право доступа к персональным данным, определяется документом «Перечень сотрудников, осуществляющих обработку персональных данных», утверждённым Руководителем Оператора. Все лица, допущенные к работе с персональными данными, подписывают обязательство о неразглашении персональных данных субъектов ПДн.

8.3. Субъект ПДн имеет право:

8.3.1. на ознакомление с документами оператора, устанавливающими порядок обработки ПДн, а также его права и обязанности в этой области;

8.3.2. отозвать согласие на обработку ПДн в установленном порядке;

8.3.3. требовать от Оператора уточнения своих ПДн, их блокирования и уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

8.3.4. получить свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн;

8.3.5. на иные права, предусмотренные законодательством Российской Федерации и локальными актами Оператора.

8.4. Субъект ПДн обязан предоставлять верные ПДн, а в случае изменений в ПДн, обнаружения ошибок или неточностей в них сообщить об этом Оператору.

8.5. Оператор обязан:

8.5.1. уведомить субъекта ПДн об обработке ПДн в случаях, если ПДн получены не от субъекта ПДн;

8.5.2. при отказе от предоставления ПНн субъекту разъяснить последствия такого отказа;

8.5.3. обеспечить неограниченный доступ к документам, определяющим политику в отношении обработки ПДн, а также реализуемых требований к защите ПДн;

8.5.4. давать ответы на запросы и обращения субъектов ПДн, их законных представителей и уполномоченного органа по защите прав субъектов ПДн.

9. Организация обработки ПДн

9.1. Получение ПДн.

9.1.1. Все ПДн следует получать непосредственно от субъекта ПДн. Субъект самостоятельно принимает решение о предоставлении своих ПДн и дает письменное согласие на их обработку Оператором.

9.1.2. В случае недееспособности либо несовершеннолетия субъекта ПДн все персональные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении ПДн своего подопечного и дает письменное согласие на их обработку оператором.

9.1.3. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случаях, указанных в пункте 9.1.2. настоящего Положения согласие может быть отозвано

законным представителем субъекта ПДн.

9.1.4. Если предоставление ПДн является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

9.1.5. В случаях, когда Оператор может получить необходимые ПДн субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие, за исключением случаев, предусмотренных законодательством или федеральными законами Российской Федерации. В согласии Оператор обязан сообщить о целях, способах и источниках получения ПДн, а также о характере подлежащих получению ПДн и возможных последствиях отказа субъекта дать письменное согласие на их получение.

9.1.6. Запрещается получать и обрабатывать ПДн субъекта о его политических, религиозных и иных убеждениях, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством или федеральными законами Российской Федерации.

9.1.7. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

9.1.8. Оператор собирает ПДн только в объёме, необходимом для достижения целей, указанных в пункте 6. настоящего Положения.

9.2. Хранение ПДн.

9.2.1. Хранение ПДн субъектов осуществляется на бумажных и электронных носителях с ограниченным доступом.

9.2.2. Хранение ПДн субъектов осуществляется структурными подразделениями оператора в соответствии с перечнями ПДн и ИСПДн, утвержденными у Оператора.

9.2.3. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением правительства РФ 15 сентября 2008 г. № 687.

9.2.4. Хранение персональных данных в автоматизированной базе данных обеспечивается защитой согласно Постановлению Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9.2.5. ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и подлежат обезличиванию или уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

9.3. Передача персональных данных.

9.3.1. При передаче ПДн субъекта Оператор обязан соблюдать следующие требования:

– не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных законодательством или иными федеральными законами Российской Федерации;

– предупредить лиц, получающих ПДн субъекта, 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. Лица, получающие ПДн субъекта,

обязаны соблюдать требования конфиденциальности, а так же требования нормативных документов, указанных в пп 1.3 настоящего Положения;

– не сообщать ПДн субъекта в коммерческих целях без его письменного согласия.

9.3.2. Случаи выдачи ПДн на бумажных носителях третьим лицам регистрируются в Журналах учета выдачи информации на бумажных носителях. Данный журнал ведется отдельно в каждом самостоятельном (структурном) подразделении лицом, назначенным распоряжением по подразделению, ответственным за его ведение. В журнал вносится только информация о фактах выдачи ПДн на бумажных носителях вне рамок процессов основной деятельности (по запросам органов прокуратуры, других правоохранительных органов, а также органов власти и федеральных служб, уполномоченных в соответствии с действующим законодательством Российской Федерации). Ведение указанного журнала возможно в электронном виде, при условии ограничения доступа в соответствии с установленным порядком распределения доступа к информационным ресурсам.

9.3.3. Оператор имеет право, во исполнение своих обязательств по работе в системе ОМС (по договору ДМС), на обмен (прием и передачу) ПДн со страховыми медицинскими организациями и территориальным фондом ОМС, на основании приказа Федерального фонда обязательного медицинского страхования от 07.04.2011 No 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования», с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа.

9.3.4. Оператор может передавать ПДн субъекта представителям соответствующих государственных органов в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27 июля 2006 года No 152-ФЗ «О персональных данных», и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями их функций.

9.3.5. В процессе передачи ПДн Оператор гарантирует, что передача осуществляется по защищённым каналам связи.

9.4. Уничтожение и блокирование персональных данных.

9.4.1. Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

9.4.2. Оператор обязан уничтожить ПДн:

– в случае отзыва субъектом ПДн согласия на обработку, в срок, не превышающий тридцати дней с даты поступления указанного отзыва, за исключением случаев, предусмотренных законодательством или федеральными законами Российской Федерации;

– если Оператор не вправе осуществлять обработку ПДн без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством Российской Федерации, в срок, не превышающий десяти рабочих дней, если обеспечить правомерность обработки ПДн невозможно.

9.4.3. Временное прекращение операций по обработке ПДн (блокирование) должно возникать по требованию субъекта ПДн при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его ПДн.

9.4.4. В случае недостоверности обрабатываемых сведений Оператор обязан уточнить ПДн в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

9.4.5. Уничтожение бумажных носителей должно осуществляться сотрудниками, допущенными к обработке ПДн, путем, не допускающим дальнейшую

возможность ознакомления с данными документами. Уничтожение информации на автоматизированных рабочих местах должно осуществляется комиссией, способами, не позволяющими осуществить восстановление данных. При уничтожении бумажных носителей допускается применение шредера классом не ниже Р-3.

10. Ответственность за нарушение требований Законодательства РФ и локальных актов Оператора в области персональных данных и их защиты.

10.1. Руководитель структурного подразделения Оператора, разрешающий доступ сотрудника к конфиденциальному документу, содержащему ПДн, несет персональную ответственность за данное разрешение.

10.2. Работники Оператора, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.

10.3. Работники Оператора, получающие доступ к ПДн, несут персональную ответственность за обеспечение конфиденциальности предоставленной им информации. Кроме того, работники Оператора, получающие для работы документы, содержащие ПДн, несут персональную ответственность за их сохранность.

11. Заключительные положения

11.1. Ознакомление работников Оператора с настоящим Положением осуществляется под роспись в листе ознакомления.

11.2. Ознакомившись с настоящим Положением, работник Оператора подтверждает, что с содержанием настоящего Положения он(-а) ознакомлен(-а), и что содержание настоящего Положения ему (ей) понятно.

11.3. Настоящее Положение вступает в силу с момента его утверждения Руководителем Оператора и действует до его отмены.

11.4. Изменения к настоящему Положению утверждаются Руководителем Оператора.

11.5. В случаях, не указанных в настоящем Положении, следует руководствоваться действующими федеральными законами и нормативными правовыми актами Российской Федерации, регулирующими порядок обработки ПДн.

11.6. Если при изменении законодательства Российской Федерации отдельные пункты Положения вступают в противоречие с ним, то эти пункты утрачивают силу, и до момента внесения изменений в документ работники Оператора руководствуются действующим законодательством Российской Федерации, при этом факт прекращения действия одного или нескольких пунктов не влияет на действие Положения в целом.