«УТВЕРЖДЕНО»
Директор

_____ Халатаев А.С.
Приказом № 2 от «01» ноября 2017г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И КЛИЕНТОВ
ООО «Многопрофильный медицинский центр «Клиника профилактики» (ООО «ММЦ «Клиника профилактики»)

Республика Башкортостан, г. Уфа

1. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными заказчиков, клиентов (субъектов персональных данных), которые обращаются в ООО «ММЦ «Клиника профилактики» (далее – Клиника, Общество) и персональными данными работников Общества, которые необходимы работодателю в связи с трудовыми отношениями.

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.06г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.06г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.04г. №98-ФЗ «О коммерческой тайне», Федеральным законом от 22.10.04г. № 125-ФЗ «Об архивном деле и Российской Федерации», указанием Федерального агентства по образованию от 22. 10. 09г. №17-187 «Об обеспечении защиты персональных данных», Федеральным законом РФ от 22.07.1993г. № 5487-1 «Основы законодательства Российской Федерации об охране здоровья граждан (в ред. от 28.09.2010г. № 243-ФЗ)».

2.Основные понятия и термины

В настоящем Положении используются следующие термины и определения:

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, адрес электронной почты, телефонный номер, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование.

Конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

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

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Клиент (субъект персональных данных) - физическое лицо (заказчик и/или клиент) потребитель услуг Общества.

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, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В рамках настоящего Положения Оператором признается Общество.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Врачебная тайна - соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Документы, содержащие персональные сведения клиента - формы медицинской и иной учетно-отчетной документации, включающие сведения о персональных данных.

Информация - сведения (сообщения, данные) независимо от формы их представления.

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

3.Персональные данные работника.

3.1 В состав персональных данных работников Общества входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, а также о предыдущих местах их работы.

3.2 Обработка персональных данных работника осуществляется на основании его письменного согласия (Приложение №1), за исключением случаев, прямо предусмотренных действующим законодательством РФ.

3.3 Комплект документов, сопровождающий процесс оформления трудовых отношений работника в Обществе при его приеме, переводе и увольнении.

3.3.1 Информация, представляемая работником при поступлении на работу в Общество, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника).

3.3.2 При оформлении работника в Учреждение работником кадрового органа заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных льготах;
- сведения о месте жительства и контактных телефонах.

3.3.3 В кадровом органе создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии

приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

3.4 Работник, как субъект персональных данных, имеет право на получение сведений:

- об операторе, о месте нахождения оператора,

- о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных,

- на подтверждение факта обработки персональных данных оператором, а также цели такой обработки;

- о способах обработки персональных данных, применяемые оператором;

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

- о перечне обрабатываемых персональных данных и источник их получения;

- о сроках обработки персональных данных, в том числе сроки их хранения;

- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;

- на ознакомление с персональным и данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

3.5 Работник имеет право:

- требовать от оператора 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;

- доступа к своим персональным данным при личном обращении к представителю Учреждения при наличии паспорта;

- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;

- оформить доверенность на право доступа к его персональным данным;

- принимать предусмотренные законом меры по защите своих прав.

4 Персональные данные клиентов.

4.1 В состав персональных данных клиентов Учреждения входят документы, содержащие информацию о паспортных данных, страховом полисе ДМС, амбулаторная карта больного, а так же иные документы сопровождающие оказание медицинских услуг.

4.2. Получение персональных данных клиента преимущественно осуществляется путем представления клиентом письменного согласия на обработку персональных данных, за исключением случаев прямо предусмотренных действующим законодательством РФ.

В случае недееспособности клиента или не достижения клиентом возраста 15 лет согласие на обработку его персональных данных дает в письменной форме его законный представитель.

В случае смерти клиента согласие на обработку его персональных данных дают в письменной форме наследники клиента, если такое согласие не было дано клиентом при его жизни.

4.3 Клиент, как субъект персональных данных, в том числе специальной категории персональных данных, имеет право па получение сведений:

- об операторе, о месте нахождения оператора;

- о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных;

- на подтверждение факта обработки персональных данных оператором, а также цели такой обработки;

- о способах обработки персональных данных, применяемые оператором;

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

- о перечне обрабатываемых персональных данных и источник их получения;

- о сроках обработки персональных данных, в том числе сроки их хранения;

- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;

- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

4.4 Клиент имеет право:

- требовать от оператора 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;

- доступа к своим Персональным данным при личном обращении к представителю Оператора при наличии паспорта;

- доступа к своим Персональным данным при направлении письменного запроса, который должен содержать помер основного документа, удостоверяющего личность субъекта Персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта Персональных данных;

- оформить доверенность на право доступа к его персональным данным;

- принимать предусмотренные законом меры по защите своих прав.

4.5 При приеме к врачу клиент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;

- страховой полис обязательного медицинского страхования;

- в отдельных случаях с учетом специфики обследования в учреждение здравоохранения действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

5. Сбор, обработка и хранение персональных данных.

5.1 Все персональные данные субъекта следует получать у него самого. Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников (медицинских карт для клиентов), которые хранятся в личном деле в отделе кадров (регистратуре/архиве). Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

5.2 Общество не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях.

5.3 Обработка персональных данных должна осуществляться на основе принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе;

- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.4 Согласие субъекта персональных данных не требуется в случаях, определенных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11, в том числе:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия Общества;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

В остальных случаях при обработке персональных данных необходимо руководствоваться ст. 6, 911 Федерального закона от 27 июля 2006 № 152-ФЗ.

5.5 Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование и адрес Общество, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- наименование и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка будет поручена такому лицу;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;

- подпись.

5.6 Запрещается требовать от лица, поступающего на работу (или прием), документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

5.7 Персональные данные субъектов хранятся в электронных базах данных и на бумажных носителях в помещении отдела кадров (регистратуре). Для этого используются специально оборудованные шкафы и сейфы. Личные дела уволенных (прошедших обследование, лечение) субъектов хранятся в архиве Общества.

5.8 В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, должность, подразделение, служебные телефоны и адрес электронной почты.

5.9 Сведения о начислении и выплате заработной платы работникам Общества хранятся в электронных базах данных и на бумажных носителях в помещении бухгалтерии. По истечении сроков хранения, установленных законодательством РФ, данные сведения передаются в архив Общества или уничтожаются.

5.10 Конкретные обязанности по ведению, хранению личных дел субъектов, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные субъектов, возлагается на работников отдела кадров и регистратуры, а по хранению личных дел уволенных (обследованных, пролеченных) субъектов на работников архива и закрепляются в должностных инструкциях.

5.11 Персональные данные клиентов хранятся в электронных базах данных, которые могут быть подключены к локальной сети организации, а так же на бумажных носителях.

5.12 Доступ к электронным базам данных ограничен паролем. Возможна передача персональных данных клиентов между структурными подразделениями с использованием учтенных съемных носителей или по внутренней сети Общества с использованием технических и программных средств защиты информации, с доступом только для работников Общества, допущенных к работе с персональными данными клиентов Приказом генерального директора и только в объеме, необходимом данным работникам для выполнения ими своих должностных обязанностей.

5.13 Бумажными носителями персональных данных являются:

- медицинская карта амбулаторного больного, которая заводится на каждого обратившегося в Клинику за оказанием медицинском помощи при первом обращении и хранится в регистратуре Клиники. Медицинская карта передается врачам-специалистам Клиники при личном обращении клиента в Клинику, по окончании приема медицинская карта сдается медсестрой врача-специалиста в регистратуру Клиники;

- медицинская карта стационарного больного, которая заводится на каждого поступившего в стационар на лечение клиента в приемном отделении стационара Клиники и хранится в течение всего срока пребывания клиента в стационаре в папке лечащего врача. В случае необходимости предоставления медицинской карты в другие подразделения Клиники для проведения по назначению лечащего врача диагностических исследований, консультаций врачей-специалистов медицинская карта до начала исследования/консультации передается постовой медсестрой отделения медицинскому персоналу соответствующего подразделения, после проведения исследований/консультаций возвращается медицинским персоналом данного подразделения лечащему врачу;

- медицинская карта больного дневного стационара при больничном учреждении, дневного стационара при амбулаторно-поликлиническом учреждении, стационара на дому;

- журналы и другие формы медицинской документации, содержащие персональные данные клиентов, оформляются и хранятся в регистратуре, кабинетах врачей Клиники в соответствии с требованиями действующих приказов;

- прочие документы, используемые при оказании медицинской помощи и содержащие персональные данные клиентов (акты, направления, договоры, квитанции и пр.), после оформления передаются работнику, допущенному к работе с персональными данными, в должностные обязанности которого входит обработка этих данных.

Хранение оконченных производством документов, содержащих персональные данные клиентов, осуществляется в архиве Общества.

5.14 Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

5.15 При получении сведений, составляющих персональные данные субъектов заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

6. Передачи персональных данных субъектов ИД

6.1 При передаче персональных данных субъектов сотрудники Общества, имеющие доступ к персональным данным, должны соблюдать следующие требования:

6.1.1 Не сообщать персональные данные субъекта третьей стороне без письменного согласия работника субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

6.1.2 Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

6.1.3 Предупредить лиц, получающих персональные данные 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.

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

7. Защита персональных данных.

7.1 Защита персональных данных в Учреждении представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права па доступ к информации.

7.2 В целях обеспечения безопасности персональных данных при их обработке в информационных системах Общества:

- установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- помещения, в которых ведется работа с персональными данными, должны обеспечивать сохранность носи телей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- доступ к информации в электронном виде должен осуществляться с использованием парольной защиты, а в информационных системах персональных данных - с использованием средств автоматизации в соответствии с нормативными документами;

- электронные носители информации, содержащие персональные данные, учитывают в журнале учета электронных носителей персональных данных.

7.3 Обеспечение безопасности персональных данных в информационных системах персональных данных осуществляется в соответствии с требованиями ст. 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

7.4 Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых Обществом угроз безопасности персональных данных (модели угроз) и в зависимости от уровня защищенности информационной системы.

7.5 Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе системы защиты персональных данных.

7.6 Сотрудники Общества, имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, граждане ко-правовую или уголовную ответственность в соответствии с действующим российским законодательством.