УТВЕРЖДАЮ

Директор ООО «МедсервисТула»

_____ А.В.Мосин

«____» _____ 20___г.

ПОЛОЖЕНИЕ ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «МедсервисТула»

1. Общее положения

1.1. Настоящее Положение по обработке персональных данных (далее –Положение) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 «О персональных данных» и является основополагающим внутренним регулятивным документом медицинской организации ООО «МедсервисТула» (далее - Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация. Настоящие положение определяет политику организации в отношении обработки персональных данных.

1.2. Положение разработан в целях реализации требований законодательства в области обработки и защиты ПДн и направлено на обеспечение защиты прав и свободы человека и гражданина при обработке его ПДНв Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положение настоящего Положения распространяются на отношения по обработке и защите ПДн, полученных организацией как до, так и после утверждения Положения, за исключением случаев, когда по причинам правового, организационного и иного характера положения настоящего Положения не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами, и определяемых:

- Федеральным законом от 21 ноября 2011 г. № 323 – ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральным законом № 152 – ФЗ от 27 июля 2006 года «О персональных данных»;

- Постановлением Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановлением Правительства РФ от 1 ноября 2012 года №1119 « Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных;

- иными нормативами правовым и актами Российской Федерации.

Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящее Положение. Новая редакция Положения вступает в силу с момента ее утверждения руководителем Организации, если иное не предусмотрено новой редакцией Положения.

2. термины и принятые сокращения

Персональные данные (ПДн)- любая информация относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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:

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), совершаемых с персональными данными;

Распространение персональных данных – действия, направленные на распространение 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 невозможном установить содержаниеперсональных 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;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Информационная система персональных данных (ИСПд) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинской экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно- противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях;

Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3.Принципы обеспечения безопасности персональных данных

3.1. 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.

3.2. Для обеспечения безопасности ПДн организация руководствуется следующими принципами:

- законность: защита ПДн основывается на положениях правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн:

- системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

- комплектность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах организации и других имеющихся в организации систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе и при проведении ремонтных и регламентных работ;

- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн принимаются до начала их обработки;

- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств индивидуальной защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

- персональная ответственность: ответственность за обеспечение безопасностиПДн возлагается на Работников в пределах их безопасностей, связанных с обработкой и защитой ПДн;

- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;

- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками и, имеющими необходимые для этого квалификацию и опыт;

- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения был и явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПДн, несовместимая с целью их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организации ПДн уничтожаются или обезличиваются.

3.4. при обработке ПДн обеспечивается их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уничтожению неполных или неточных ПДн.

4. Обработка персональных данных

4.1. Получение ПДн

4.1.1. Документы, содержащие ПДн создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесение сведений в учетные формы;

в) получение оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика идр.).

Доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством РФ и осуществляется только по заявлению субъекта ПДн либо его представителя (законного представителя).

4.2. Обработка ПДн

4.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку егоперсональных данных;

- в случаях, когда обработка персональных данных необходима для исполнения полномочий федеральных законов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210- ФЗ « Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъектаперсональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

- в случаях, когда обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

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

-в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее- персональные данные, сделанные общедоступными субъектом персональных данных). Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями регулятивных документов организации.

Допущенные к работе ПДн работники знакомятся с локальными нормативными актами Организации в сфере обработки и защиты конфиденциальности персональных данных и положениями законодательства Российской Федерации в сфере обработки и защиты персональных данных.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.2.2. Цели обработки ПДн:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 323-ФЗ « Об основах охраны здоровья граждан

Российской Федерации», от 12 апреля 2010г. №61-ФЗ « Об обращении лекарственных средств», Правилам и предоставления медицинским и организациями платных услуг, утвержденными Постановлением Правительства Российской Федерации и от 4 октября 2012г. №1006;

- осуществление трудовых отношений;

- осуществление гражданского-правовых отношений.

- 4.2.3. категории субъектов персональных данных

В Организации обрабатывают ПДн следующих субъектов:

- физические лица, состоящие с организацией в трудовых отношениях;

- физические лица, являющие близкими родственниками сотрудников организации;

- физические лица. Уволившиеся из организации;

- физические лица, являющиеся кандидатами на работу;

- физические лица, состоящие с организацией в гражданско- правовых отношениях;

- физические лица, обратившиеся в организацию за медицинской помощью и иными услугами.

4.2.4. ПДн, обрабатываемые Организацией:

-данные, полученные при осуществлении трудовых отношений;

-данные, полученные для осуществления отбора кандидатов на работу в организацию;

-данные, полученные при осуществлении гражданско-правовых отношений;

-данные, полученные при оказании медицинской помощи и иных услуг.

4.2. Обработка персональных данных ведется:

- с использованием средств автоматизации;

- без использования средств автоматизации.

4.3. Хранение ПДн:

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа (архив).

4.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих Пд, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение ПДн

4.4.1. Уничтожение документов (носителей), содержащих ПДн производится путем стюкения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПДн на электронных носителях уничтожаются путем стирания или формирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

4.5. Передача ПДн

4.5.1. Организация передает ПДн третьим лицам в следующих случаях:

- субъект выразил согласие на такие действия;

- передача предусмотрена законодательством РФ;

4.5.2. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

-Пенсионный фонд РФ для учета (в Случаях, установленных действующим законодательством РФ);

- Налоговые органы РФ (в случаях, установленных действующим законодательством РФ);

- Фонд социального страхования (в случаях, установленных действующим законодательством РФ);

- Территориальный фонд обязательного медицинского страхования (в случаях, установленных действующим законодательством РФ);

- страховые медицинские организации по обязательному медицинскому страхованию (в случаях, установленных действующим законодательством РФ);

- банки для начисления заработной платы (в случаях, установленных действующим законодательством РФ);

- судебные и правоохранительные органы в случаях, установленных законодательством;

- в иные органы и организации только в случаях, установленных действующим законодательством РФ или с согласия субъекта персональных данных.

5. Защита персональных данных.

5.1. В соответствие с требованиями и нормативных документов Организацией создана система защитыперсональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно- распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно- аппаратных средств, обеспечивающих защиту ПДн.

5.5. Основными мерами защиты ПДн, используемыми Организацией, являются:

5.5.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;

5.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИС ПД, и разработка мер и мероприятий по защите ПДн;

5.5.3. Разработка Положения по обработке и защите персональных данных;

5.5.4. Установление правил доступа к ПДн, обрабатываемым в ИС ПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн и в ИСПД;

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;

5.5.7. Сертифицированный межсетевой экран и средство обнаружения вторжения;

5.5.8. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

5.5.9. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

5.5.10. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.5.11. Ознакомление работников Организации и непосредственно осуществляющих обработку персональных данных с положениями законодательства Российской Федерации в сфере обработки и защиты конфиденциальностиперсональных данных, локальными нормативными актами Организации в сфере обработки и защиты конфиденциальности персональных данных;

5.5.12. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПДн и обязанности Организации

6.1. Основные права субъекта ПДн

Субъект ПДн имеет право на получение информации, касающейся обработки егоперсональных данных, в том числе содержащей:

- подтверждение фактов обработки персональных данных оператором;

- правовые основания и цели обработки персональных данных;

- цели и применяемые оператором способы обработки персональных данных;

-наименование и место нахождения оператора, сведения о лицах (за исключением работников операторов), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

-порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

-иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются не полными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности Организации

6.1. Организация обязана:

-при сборе ПДн предоставить информацию об обработке его ПДн;

-в случаях если ПДн были получены не от субъекта ПДн, уведомить субъекта;

- при отказе субъекта в предоставлении ПДн Организацией субъекту разъясняются последствия такого отказа;

-опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемыхтребованиях к защите ПДн;

-принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

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