УТВЕРЖДАЮ
Главный врач
ООО «Виталиния-М»

_____ / Ю.В. Беляева
«14» сентября 2020 г.
М.П.

ПОЛИТИКА
в отношении обработки и обеспечения безопасности персональных данных
в обществе с ограниченной ответственностью «Виталиния-М»

1. Общие положения

1.1. Назначение политики

Настоящая Политика в отношении обработки и обеспечения безопасности персональных данных (далее – ПДн) в обществе с ограниченной ответственностью «Виталиния-М» (далее – Политика) разработана в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн и определяет цели и общие принципы обработки ПДн, а также реализуемые меры защиты персональных данных в обществе с ограниченной ответственностью «Виталиния-М» (далее – Учреждение).

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

Политика является общедоступным документом и предусматривает возможность ознакомления с ней неограниченного круга лиц.

1.2. Основные понятия

В Политике используются следующие основные понятия:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

оператор 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), совершаемые с персональными данными;

обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

– сбор;
– запись;
– систематизацию;
– накопление;
– хранение;

– уточнение (обновление, изменение);
– извлечение;
– использование;
– передачу (распространение, предоставление, доступ);
– обезличивание;
– блокирование;
– удаление;
– уничтожение.

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

распространение персональных данных – действия, направленные на раскрытие 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 невозможным восстановить содержание персональных 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;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3 Основные права и обязанности Оператора и субъекта ПДн

1.3.1 Основные права Оператора

Учреждение как Оператор персональных данных вправе:

– отстаивать свои интересы в суде;

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

– отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

– использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством;

– проверять полноту и точность предоставленных персональных данных.

В случае выявления ошибочных или неполных персональных данных, имеет право прекратить все отношения с субъектом персональных данных, если это не противоречит законодательству.

1.3.2 Основные обязанности Оператора

Учреждение как Оператор персональных данных обязано:

– принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных» (далее – закон о персональных данных) и принятыми в соответствии с ним нормативными правовыми актами. Учреждение самостоятельно определяет состав, и перечень необходимых мер;

– предоставить субъекту персональных данных по его просьбе следующую информацию:

1) подтверждение факта обработки персональных данных Учреждением;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Учреждением способы обработки персональных данных;

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

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

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных законом о персональных данных;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные законом о персональных данных или другими федеральными законами.

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, работники в Учреждении обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Учреждение не собирает персональные данные, не обрабатывает и не передает персональные данные субъектов персональных данных третьим лицам, без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.3.3 Основные права субъекта

Субъект персональных данных имеет право:

– требовать 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;

– требовать перечень своих персональных данных, обрабатываемых Учреждением и источник их получения;

– получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

– требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

– на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

– получить сведения, касающиеся обработки его персональных данных Учреждением;

– потребовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

2. Цели сбора персональных данных

Обработка ПДн в Учреждении предусматривает следующие цели:

– оказание экстренной, неотложной, консультативной, диагностической, профилактической и лечебной медицинской помощи населению, установления медицинского диагноза субъекта ПДн, оказания медицинских, медико-профилактических и медико-социальных услуг субъекту ПДн; оказание услуг населению по записи на прием к врачу в электронном виде; проведение профилактической и санитарно-информационной работы среди населения, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 04.10.2012 г. № 1006;

– ведение кадрового учета и личных дел, охрана труда и здоровья проверка профессиональной пригодности; воинский учет; реализация

социальной политики в отношении работников Учреждения;

– рассмотрение обращений граждан, поступивших в Учреждение;

– исполнения обязательств по договорам с субъектом ПДн (договоры гражданско-правового характера).

3. Правовые основания обработки персональных данных

Персональные данные обрабатываются в Учреждении на основании и в соответствии со следующими нормативно-правовыми актами:

– Конституцией Российской Федерации от 25.12.1993г.;

– Трудовым кодексом Российской Федерации от 30.12.2001 г. № 197-ФЗ;

– Гражданским кодексом Российской Федерации от 30.11.1994 г. № 51-ФЗ;

– Налоговым кодексом Российской Федерации от 31.07.1998 г. № 146-ФЗ;

– Федеральным законом от 19.12.2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

– Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Федеральным законом от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

– Федеральным законом от 29.12.2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

– Федеральным законом от 12.04.2010 г. № 61-ФЗ «Об обращении лекарственных средств»;

– Федеральным законом от 30.04.2008 г. № 56-ФЗ «О дополнительных страховых взносах на накопительную пенсию и государственной поддержке формирования пенсионных накоплений»;

– Федеральным законом от 15.12.2001 г. № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

– Постановлением Госкомстата Российской Федерации от 05.01.2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

– Приказом Федерального фонда ОМС от 7.04.2011 г. № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования»;

– Постановлением Фонда социального страхования РФ от 10.02.2010 г. № 31 «Об утверждении форм заявки на финансовое обеспечение расходов на выплату отдельных видов государственных пособий и отчета о расходовании

средств, предусмотренных на финансовое обеспечение расходов на выплату отдельных видов государственных пособий лицам, не подлежащим обязательному социальному страхованию на случай временной нетрудоспособности и в связи с материнством, а также уволенным (прекратившим деятельность, полномочия) в установленном порядке»;

– Приказом Министерства здравоохранения РФ от 30.01.2015 г. № 29н «О формах статистического учета и отчетности, используемых при организации оказания высокотехнологичной медицинской помощи с применением специализированной информационной системы, порядках их заполнения и сроках представления»;

– Приказом Министерства здравоохранения РФ от 15.12.2014 г. № 834н «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению»;

– Порядком ведения персонифицированного учета в сфере обязательного медицинского страхования, утвержденного приказом Минздравсоцразвития России от 25.01.2011 № 29н;

– лицензией на осуществление медицинской деятельности;

– уставом Учреждения;

– договорами с контрагентами;

– внутренними документами в области защиты персональных данных.

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Сведениями, составляющими персональные данные, в Учреждении является любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). В состав обрабатываемых в Учреждении персональных данных пациентов и работников могут входить:

– фамилия, имя, отчество;

– пол;

– дата рождения или возраст;

– паспортные данные (для подписания договора оказания услуг, согласия на предоставление и обработку персональных данных и трудового договора);

– адрес проживания;

– номер телефона, факса, адрес электронной почты (по желанию);

– информация о состоянии здоровья;

– другая информация, необходимая для правильного проведения и интерпретации медицинских исследований;

– результаты выполненных медицинских исследований;

– другая информация, необходимая для выполнения обязательств организации в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, законодательством об обязательных видах

страхования, со страховым законодательством.

Учреждение осуществляет обработку данных о состоянии здоровья пациентов в целях оказания медицинских услуг, установления медицинского диагноза при этом обработка персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Учреждение осуществляет обработку данных о состоянии здоровья работников в соответствии с трудовым законодательством Российской Федерации.

4.2 Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

– работников, состоящих с Учреждением в трудовых отношениях;

– физических лиц, в отношении которых в Учреждении оказана медицинская помощь;

– физических лиц, обратившихся в Учреждение за медицинской помощью

– физических лиц, являющихся близкими родственниками сотрудников учреждения;

– физических лиц, уволившихся из Учреждения;

– физических лиц, являющихся кандидатами при устройстве на работу;

– физических лиц, состоящих с учреждением в гражданско-правовых отношениях.

5. Порядок и условия обработки персональных данных

В Учреждении осуществляются следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработка персональных данных осуществляется:

– с согласия субъекта персональных данных на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения, возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

– 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 Учреждения к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке ПДн работники Учреждения под роспись

знакомятся с документами, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных его работников.

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

Обработка персональных данных ведется:

– с использованием средств автоматизации;

– без использования средств автоматизации.

5.1 Хранение ПДн

ПДн субъектов могут передаваться на хранение как на бумажных носителях, так и в электронном виде.

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

ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках) и базах данных доступ к которым предоставляется согласно матрицы доступа утвержденной руководителем Учреждения.

Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в локально-вычислительной сети Учреждения.

Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки и подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении за исключением случаев, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.2 Уничтожение ПДн

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

ПДн на электронных носителях уничтожаются путем стирания, перезаписи данных и форматирования носителя.

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

5.3 Передача ПДн

Передача Пдн Учреждением осуществляется только с применением соответствующих мер и средств защиты информации.

Учреждение передает ПДн третьим лицам в следующих случаях:

– субъект выразил свое согласие на такие действия;

– передача предусмотрена российским или иным применимым

законодательством в рамках установленной законодательством процедуры.

На законных основаниях осуществляется передача ПДн в:

– Министерство здравоохранения Ставропольского края;

– Государственное бюджетное учреждение Ставропольского края «Медицинский информационно аналитический центр»

– Пенсионный фонд РФ;

– Налоговые органы РФ;

– Управление Федерального казначейства по Ставропольскому краю;

– Фонд социального страхования;

– Территориальный фонд обязательного медицинского страхования;

– страховые медицинские организации по обязательному и добровольному медицинскому страхованию;

– банки для начисления заработной платы (на основании договора);

– судебные и правоохранительные органы в случаях, установленных законодательством;

– Военный комиссариат

В остальных случаях передача ПДн может осуществляться только с согласия субъекта персональных данных.

5.4 Обеспечение безопасности ПДн

Обеспечение безопасности персональных данных Учреждением достигается, в частности следующими мерами:

– оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения закона «О персональных данных», соотношение указанного вреда и принимаемых защитных мер;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных закону «О персональных данных» и внутренним документам Учреждения по вопросам обработки персональных данных;

– ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, и разработанными в Учреждении политикой в отношении обработки персональных данных, локальными актами по вопросам обработки и защиты персональных данных, и (или) обучение указанных работников;

– учет машинных носителей персональных данных;

– восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– назначение ответственного за организацию обработки персональных данных;

– применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (сертифицированные СЗИ);

– определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной

системы персональных данных;

– установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

– контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

– базы персональных данных Учреждения находятся полностью в пределах территории Российской Федерации.

При обработке персональных данных, осуществляемой без использования средств автоматизации, в Учреждении выполняются требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.5 Регламент реагирования на запросы обращения субъектов персональных данных и их представителей

В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат актуализации их Учреждением, а обработка должна быть прекращена, соответственно.

При обращении, запросе в письменной или электронной форме субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Учреждение руководствуется требованиями статей 14, 18 и 20 Федерального закона № 152-ФЗ;

Субъект или его законный представитель может воспользоваться формами запросов, указанными в приложениях 1-3 к данной Политике.

Доступ субъекта персональных данных или его законного представителя к своим персональным данным Учреждение предоставляет только под контролем ответственного за организацию обработки персональных.

Обращение, запрос в письменной или электронной форме субъекта персональных данных или его законного представителя фиксируются в журнале учета запросов и обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

Ответственный за организацию обработки персональных данных в Учреждении принимает решение о предоставлении доступа субъекта к персональным данным.

В случае, если данных предоставленных субъектом недостаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся

основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает (ов) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения.

Сведения о наличии персональных данных Учреждение предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

Сведения о наличии персональных данных предоставляются субъекту при ответе на запрос в течение тридцати дней от даты получения запроса субъекта персональных данных или его законного представителя.

5.6 Регламент реагирования на запросы обращения уполномоченных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников Учреждения.

В течение установленного срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.