Приложение №1
к приказу от 14.04.2016 № 195

ПОЛИТИКА
Территориального фонда обязательного медицинского страхования Пензенской области в отношении обработки персональных данных

1. Общие положения

Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее Закон № 152-ФЗ) в целях обеспечения информационной безопасности при работе с персональными данными и соблюдения законных интересов граждан, являющихся субъектами персональных данных, обрабатываемых в Территориальном фонде обязательного медицинского страхования Пензенской области (далее - ТФОМС) и определяет политику ТФОМС в отношении обработки персональных данных (далее - Политика), а так же содержит сведения о реализуемых требованиях к защите обрабатываемых персональных данных. Соблюдение правил и принципов Политики является обязательным в ТФОМС.

Основные понятия, используемые в Политике:

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

-конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

-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;

-информационная система персональных данных (ИСПДн) – 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.

Основные обязанности оператора персональных данных:

-при сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»;

-если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

-оператор обязан соблюдать конфиденциальность персональных данных, если иное не предусмотрено федеральным законом;

-при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»;

-оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;

-оператор, являющийся юридическим лицом, обязан назначить лицо, ответственное за организацию обработки персональных данных;

-оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя, либо в случае отказа дать письменный мотивированный ответ;

-оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

-в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных

данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

-в случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных;

-в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;

-в случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами;

-в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных

без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами;

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

- оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Права оператора персональных данных:

- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;

-использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством Российской Федерации;

-предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством Российской Федерации (в правоохранительные органы и др.);

-оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных .данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных».

Права субъекта персональных данных:

-субъект персональных данных имеет право на доступ к его персональным данным, если данное право не ограничено в соответствии с федеральными законами;

-субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, если данное право не ограничено в соответствии с федеральными законами;

-если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований законодательства РФ или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

-субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

2. Цели обработки персональных данных

Обработка персональных данных в ТФОМС осуществляется в следующих целях:

-реализация государственной политики в области обязательного медицинского страхования граждан, как составной части государственного социального страхования;

-реализация трудового законодательства Российской Федерации в отношении работников ТФОМС, ведения кадрового и бухгалтерского учета;

-формирование общедоступных источников персональных данных (справочников, адресных книг);

-организация пропускного режима;

-реализация гражданином Российской Федерации закрепленного за ним Конституцией Российской Федерации права на обращение в государственные органы.

3. Правовые основания обработки персональных данных

В качестве правового основания обработки персональных данных в ТФОМС служат:

-Федеральный закон от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

-Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

-Налоговый кодекс Российской Федерации;

-Трудовой кодекс Российской Федерации;

-Федеральный закон от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

-согласие субъекта персональных данных на обработку персональных данных.

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

К категориям субъектов персональных данных в ТФОМС относятся:

- лица застрахованные в системе обязательного медицинского страхования (специальные категории, включающие сведения о состоянии здоровья более 100 000 субъектов);

- лица, которые участвуют в оказании медицинских услуг (персональные данные медицинского персонала в рамках системы обязательного медицинского страхования, менее 100 000 субъектов);

-лица, работающие или работавшие в ТФОМС Пензенской области (менее 100 000 субъектов, в том числе специальные категории, включающие сведения о национальной принадлежности);

-лица являющиеся близкими родственниками работников ТФОМС Пензенской области (менее 100 000 субъектов);

- посетители ТФОМС (менее 100 000 субъектов).

Категории обрабатываемых персональных данных застрахованных в системе обязательного медицинского страхования лиц: фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; страховой номер индивидуального лицевого счета (СНИЛС); данные о страховой медицинской организации, выбранной застрахованным лицом; дата регистрации в качестве застрахованного лица; статус застрахованного лица (работающий, неработающий); номер полиса обязательного медицинского страхования застрахованного лица; сведения о медицинской организации, оказавшей медицинские услуги; виды оказанной медицинской помощи; условия оказания медицинской помощи; формы оказания медицинской помощи; сроки оказания медицинской помощи; объемы оказанной медицинской помощи; стоимость оказанной медицинской помощи; диагноз; профиль оказания медицинской помощи; сведения о медицинских услугах, оказанных застрахованному лицу, и о примененных лекарственных препаратах; примененные стандарты медицинской помощи; сведения о медицинском работнике или медицинских работниках, оказавших медицинские услуги; результат обращения за медицинской помощью.

Категории обрабатываемых персональных данных лиц, которые участвуют в оказании медицинских услуг (персональные данные медицинского персонала в рамках системы ОМС), в том

числе: фамилия, имя, отчество (последнее - при наличии); пол; дата рождения; место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования; сведения об образовании, в том числе данные об образовательных организациях и о документах об образовании и (или) о квалификации; наименование организации, оказывающей медицинские услуги; занимаемая должность в организации, оказывающей медицинские услуги.

Категории обрабатываемых персональных данных работников ТФОМС: фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство; данные документа, удостоверяющего личность; место жительства; место регистрации; дата регистрации; реквизиты страхового Свидетельства государственного пенсионного страхования; сведения о воинском учете и реквизиты документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу); сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании); анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе - автобиография); сведения, содержащиеся в иных документах, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (например, медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров); сведения, содержащиеся в трудовом договоре; сведения, содержащиеся в личной карточке по форме Т-2; номер контактного телефона или сведения о других способах связи; сведения о семейном положении; сведения о прохождении работником аттестации, собеседования, повышения квалификации; сведения о работнике, нахождение которых в личном деле работника необходимо для корректного документального оформления трудовых правоотношений с работником; сведения о доходах.

Категории обрабатываемых персональных данных близких родственников работников ТФОМС: ФИО, год рождения.

Категории обрабатываемых персональных данных посетителей ТФОМС: фамилия, имя, отчество, место работы, время прибытия, время убытия;

5. Порядок и условия обработки персональных данных

В ТФОМС используется смешанный (с использованием средств автоматизации и без использования средств автоматизации) способ обработки персональных данных с передачей информации по внутренней локальной сети и с передачей информации по сети Интернет в защищенном виде.

Обработка персональных данных в ТФОМС осуществляется путем следующих операции с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

Трансграничная передача персональных данных не производится. Обработка персональных данных происходит с использованием баз данных, находящихся на территории Российской Федерации.

Обработка персональных данных в ТФОМС осуществляется на основании следующих принципов:

-законности и справедливости целей и способов обработки персональных данных;

-соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям ТФОМС;

-соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

-хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

-уничтожения либо обезличивания по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

Передача персональных данных, обрабатываемых ТФОМС, другим организациям, третьим лицам осуществляется в случаях и в порядке предусмотренных законодательством РФ

В ТФОМС соблюдаются требование конфиденциальности в отношении персональных данных: оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

В ТФОМС принимаются необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в соответствии с требованиями законодательства Российской Федерации:

-назначен, приказом ТФОМС, ответственный за организацию обработки персональных данных;

-назначен, приказом ТФОМС, ответственный за обеспечение безопасности персональных данных;

-определена контролируемая зона, обеспечиваются, пропускной и внутриобъектовый режимы;

-определен перечень сведений конфиденциального характера и перечень лиц, имеющих доступ к ней;

- определены угрозы безопасности, в том числе персональных данных;

- ведется учет машинных носителей персональных данных;

- проводится ознакомление работников ТФОМС, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ТФОМС в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

-установлены правила доступа к персональным данным, как с использованием средств автоматизации, так и без их использования;

-обеспечены регистрация и учет действий, совершаемых с персональными данными в информационной системе персональных данных;

-организовано конфиденциальное делопроизводство;

-обработка сведений конфиденциального характера осуществляется в специальных помещениях, для которых установлен особый порядок доступа;

-организованы хранилища для хранения конфиденциальной информации на материальных носителях;

-хранение персональных данных граждан производится с использованием баз данных, находящихся на территории Российской Федерации;

-организована и контролируется работа со средствами криптографической защиты информации (назначен ответственный пользователь криптографических средств, ведется поэкземплярный учет средств криптографической защиты информации, защита персональных данных с использованием средств криптографической защиты информации осуществляется в специальных помещениях с установленным режимом доступа);

-применяется система защиты информации от несанкционированного доступа к информации, построенная на основе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

-используется антивирусное программное обеспечение;

- производится резервное копирование необходимых информационных ресурсов и имеется возможность восстановления персональных данных;

- установлен уровень защищенности персональных данных в ТФОМС, принимаются все необходимые меры, предъявляемые к защите персональных данных для установленного уровня, в соответствии с требованиями нормативных документов (в том числе нормативных документов утвержденных Правительством РФ, ФСТЭК и ФСБ РФ);

- не реже одного раза в год проводится внутренний контроль и (или) аудит соответствия обработки персональных данных требования законодательства РФ согласно приказу ТФОМС;

- осуществляется регулярный контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных (постоянный контроль проводят администратор системы защиты; лицо, ответственное за обеспечение безопасности персональных данных; лицо, ответственное за организацию обработки персональных данных; ответственный пользователь средств криптографической защиты информации: лицо, ответственное за конфиденциальное делопроизводство) ;

- на ИСПДн ТФОМС выдан аттестат соответствия требованиям по безопасности информации, подтверждающий эффективность принимаемых мер по обеспечению безопасности персональных данных.

ТФОМС прекращает обработку персональных данных в случаях:

-достижения цели обработки персональных данных либо утраты необходимости в достижении этой цели;

-выявления неправомерных действий с персональными данными и невозможностью устранения допущенных нарушений в срок, установленный законодательством;

-отзыва субъектом персональных данных согласия на обработку его персональных данных, в случаях, когда обработка персональных данных допускается исключительно с согласия субъекта персональных данных;

-изменения нормативных правовых актов, устанавливающих правовые основания обработки персональных данных.

Конкретные сроки хранения тех или иных категорий персональных данных зависят от положений законодательства, действующих в текущий момент времени.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

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

При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

-иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

-оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или иными федеральными законами;

-иное не предусмотрено иным соглашением между оператором и субъектом 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 действующим законодательством.

Уничтожение персональных данных осуществляется в порядке и сроки, предусмотренные законодательством РФ.

Сроки и порядок рассмотрения запросов (обращений) субъектов персональных данных в ТФОМС Пензенской области определяются в соответствии со статьями 19, 20 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных».

Для направления запросов и обращений в ТФОМС Пензенской области можно использовать следующую контактную информацию (при запросе необходимо указывать контактные данные субъекта для возможности направления ответа):

Территориальный фонд обязательного медицинского страхования Пензенской области (ТФОМС Пензенской области), расположен по адресу: г. Пенза, ул. Крупской, д. 3, 410039.

ОГРН: 1025801217397

ИНН: 5835004660

КПП: 583501001

Адрес электронной почты: tfoms@sura.ru

Контактный телефон: (8412)42-78-01

Данная политика подлежит опубликованию на официальном сайте ТФОМС www.omspenza.ru, раздел «Политика в отношении обработки ПДн».