УТВЕРЖДЕНО

приказом ТФОМС НСО
от «__»_____2015 №_____

ПОЛОЖЕНИЕ
об обработке персональных данных в информационных системах персональных данных Территориального фонда обязательного медицинского страхования Новосибирской области

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее – Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и другого использования персональных данных, обрабатываемых в информационной системе персональных данных обязательного медицинского страхования Новосибирской области (далее – ИСПДн ОМС НСО) и информационной системе персональных данных бухгалтерии и кадров Территориального фонда обязательного медицинского страхования Новосибирской области (далее – ИСПДн бухгалтерии и кадров ТФОМС НСО) в соответствии с законодательством Российской Федерации.

1.2. Настоящее Положение разработано в соответствии с:

1) Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

2) Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) Федеральным законом от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

1.3. Для целей настоящего Положения используются следующие основные понятия:

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

2) 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;

3) 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;

4) 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;

5) использование персональных данных – действия с персональными данными, совершаемые работниками Территориального фонда обязательного медицинского страхования Новосибирской области (далее – ТФОМС НСО или Оператор) в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

6) автоматизированная обработка – обработка данных, выполняемая средствами вычислительной техники;

7) блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

8) 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;

9) обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных – система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

11) защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном субъекте персональных данных.

1.4. Положение разработано 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 ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО.

1.5. Персональные данные, обрабатываемые в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО, относятся к конфиденциальной информации, порядок работы с которой регламентирован Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» и осуществляется с соблюдением строго определенных правил и условий.

2. Персональные данные, обрабатываемые в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО

2.1. Оператор обрабатывает:

1) ПДн, поступающие от субъектов и участников обязательного медицинского страхования и необходимые для осуществления функций и полномочий Оператора в соответствии с законодательством, регулирующим деятельность в сфере обязательного медицинского страхования;

2) ПДн физических лиц, находящихся в договорных и иных гражданско-правовых отношениях с оператором; сотрудников; близких родственников сотрудников, не достигших 18 лет;

3) ПДн, поступающие к Оператору в иных случаях, предусмотренных нормативными правовыми актами.

3. Обработка и защита персональных данных

3.1. Оператор осуществляет автоматизированную и неавтоматизированную обработку ПДн.

3.2. Оператор получает персональные данные только способами, предусмотренными действующим законодательством Российской Федерации.

3.3. При обработке ПДн Оператор должен соблюдать следующие требования:

1) обрабатывать ПДн работников только с их письменного согласия (приложение 1). При этом получение письменного согласия, а также разъяснение субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение, возлагается на Оператора;

2) разрешать доступ к ПДн только тем работникам, которым доступ необходим для выполнения своих служебных обязанностей в соответствии с «Перечнем информационных систем персональных данных и персональных данных, обрабатываемых в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС

НСО» (приложение 2) и «Перечнем подразделений и лиц, допущенных к персональным данным, обрабатываемым в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО»;

3) работники Оператора, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности;

4) обработка персональных данных должна осуществляться только в заявленных целях и в заявленных объемах в соответствии с «Перечнем информационных систем персональных данных и персональных данных, обрабатываемых в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО»;

5) при определении объема и содержания, обрабатываемых персональных данных, Оператор должен руководствоваться Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными федеральными законами в области защиты персональных данных;

6) при принятии решений, затрагивающих интересы субъекта ПДн, Оператор не должен основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) обработка персональных данных должна осуществляться в соответствии с «Правилами обработки персональных данных в информационных системах персональных данных Территориального фонда обязательного медицинского страхования Новосибирской области» (приложение 3).

3.4. Для обеспечения защиты ПДн при обработке в информационных системах персональных данных Оператор обязан проводить следующие мероприятия:

1) назначать должностное лицо, ответственное за организацию обработки персональных данных, которое действует в пределах своих полномочий в соответствии с «Инструкцией ответственного за организацию обработки персональных данных в информационных системах персональных данных Территориального фонда обязательного медицинского страхования Новосибирской области» (приложение 4);

2) соблюдать порядок получения, учета и хранения ПДн;

3) издавать документы, определяющие политику Оператора в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;

4) принимать правовые, организационные и технические меры по обеспечению безопасности ПДн;

5) обеспечить защиту доступа к электронной базе данных, содержащей ПДн, обеспечивается путем использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн

(средство защиты информации от несанкционированного доступа, межсетевой экран, антивирусное средство, средство обнаружения вторжений, средство защиты среды виртуализации);

6) осуществлять внутренний контроль соответствия обработки ПДн законодательству Российской Федерации;

7) ограничивать доступ в помещения, в которых ведется обработка персональных данных, в соответствии с «Порядком доступа работников ТФОМС НСО в помещения, в которых ведется обработка персональных данных и расположены средства криптографической защиты информации» (приложение 5);

8) применять технические средства охраны и сигнализации;

9) со всех работников, связанных с получением, обработкой и защитой ПДн, брать обязательство работника ТФОМС НСО о неразглашении персональных данных и о прекращении обработки персональных данных в случае расторжения с ним трудового договора (приложение 6);

10) ознакомить всех работников, связанных с получением, обработкой и защитой персональных данных субъектов ПДн, под роспись в «Журнале ознакомления работников ТФОМС НСО с документами, определяющими политику ТФОМС НСО в отношении обработки и защиты персональных данных» (приложение 7) с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, с данным Положением;

11) привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн;

12) запрещать допуск к ПДн работникам Оператора, не включенным в «Перечень подразделений и лиц, допущенных к персональным данным, обрабатываемым в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО»;

13) разрешать копирование и получение выписок персональных данных субъектов ПДн исключительно в служебных целях с письменного разрешения руководителя.

4. Хранение персональных данных

4.1. Сведения о субъектах ПДн в ТФОМС НСО на бумажных носителях должны храниться в специально оборудованных шкафах и сейфах, запирающихся на ключ и опечатывающихся. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, должны находятся у ответственных работников.

4.2. Обязанности по организации хранения сведений о субъектах ПДн,

заполнения, хранения и выдачи документов, содержащих персональные данные, в ИСПДн ОМС НСО и ИСПДн бухгалтерии и кадров ТФОМС НСО должны быть возложены на ответственного за организацию обработки персональных данных.

4.3. Маркировать и учитывать в журнале регистрации, учета и выдачи сменных носителей персональных данных съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн.

4.4. Обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений в процессе хранения персональных данных субъектов ПДн.

5. Уничтожение персональных данных

5.1. При необходимости уничтожения персональных данных Оператор должен руководствоваться следующими требованиями:

1) уничтожение персональных данных должно осуществляться комиссией по проведению мероприятий по защите персональных данных;

2) комиссия по проведению мероприятий по защите персональных данных должна осуществлять систематический контроль и выделение персональных данных, подлежащих уничтожению;

3) уничтожать бумажные носители персональных данных при помощи специального оборудования (измельчителя бумаги);

4) уничтожать персональные данные, представленные в электронном виде, специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных;

5) уничтожать персональные данные на электронных носителях путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удаления с электронных носителей методами и средствами гарантированного удаления остаточной информации;

6) уничтожать персональные данные в срок, не превышающий трех рабочих дней с даты достижения целей обработки, если иное не предусмотрено федеральными законами;

7) после окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

6. Внутренние проверки состояния защищенности информационной системы персональных данных

6.1. Проверка состояния защищенности ИСПДн должна осуществляться

комиссией по проведению мероприятий по защите персональных данных.

6.2. Проверка состояния защищенности ИСПДн осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых ТФОМС НСО, требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты персональных данных.

6.3. Проверка состояния защищенности ИСПДн должна включать в себя:

1) определение характера циркулирующих персональных данных и установленных в ИСПДн режимов их обработки;

2) определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники;

3) анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия);

4) проверку наличия сертифицированных средств защиты от вредоносных программ и вирусов (антивирусных средств защиты);

5) проверку состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);

6) проверку состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

6.4. Внутренняя проверка Комиссии по проведению мероприятий по защите персональных данных должна завершаться подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки состояния защищенности ИСПДн.

6.5. Акт должен содержать:

1) дату, время и место составления акта;

2) дату и место проведения проверки;

3) сведения о результатах проверки, в том числе о выявленных нарушениях и их характере;

4) достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их

устранению с указанием конкретных сроков.

7. Обязанности субъекта персональных данных и оператора

7.1. В целях обеспечения достоверности персональных данных субъект ПДн обязан:

1) предоставлять Оператору полные и достоверные данные о себе;

2) в случае изменения своих персональных данных сообщать данную информацию Оператору.

7.2. Оператор обязан:

1) осуществлять защиту персональных данных субъекта ПДн;

2) вести Журнал учета обращений субъектов персональных данных по вопросам обработки их ПДн в ИСПДн ТФОМС НСО;

3) ограничить доступ с помощью соответствующего средства защиты информации к Журналу учета обращений субъектов персональных данных по вопросам обработки их ПДн в ИСПДн ТФОМС НСО (в электронной и бумажной форме) кругом должностных лиц (работников), которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

4) обеспечивать хранение документации, содержащей персональные данные субъектов ПДн, при этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

8. Права субъекта персональных данных в целях защиты персональных данных

8.1. Субъект персональных данных вправе требовать от Оператора 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, а также принимать предусмотренные законом меры по защите своих прав.

8.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Оператором способы обработки персональных данных;

4) сроки обработки персональных данных, в том числе сроки их хранения.

8.3. Субъект персональных данных имеет право на определение представителей для защиты своих персональных данных.

8.4. Субъект персональных данных имеет право требовать исключить или исправить неверные или неполные персональные данные, а также данные, обрабатываемые с нарушением требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

8.5. Субъект персональных данных имеет право требовать об извещении ТФОМС НСО всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.6. Субъект персональных данных имеет право на обжалование в судебном порядке любых неправомерных действий или бездействии Оператора при обработке и защите его персональных данных.

9. Реагирование на запросы субъектов персональных данных и их законных представителей

9.1. При рассмотрении запросов, поступающих от субъектов ПДн и их законных представителей, ТФОМС НСО руководствуется «Правилами рассмотрения запросов субъектов персональных данных или их представителей по поводу обработки их персональных данных в информационных системах персональных данных Территориального фонда обязательного медицинского страхования Новосибирской области» (приложение 8).

9.2. 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.

10. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта

10.1. Лица, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

10.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.