ТЕРРИТОРИАЛЬНЫЙ ФОНД ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ САРАТОВСКОЙ ОБЛАСТИ
(ТФОМС Саратовской области)

ПРИКАЗ

13.09.2013 № 136

г. Саратов

Об утверждении Требований по подключению участников системы ОМС к ИСПДн и УЦКУ ТФОМС Саратовской области

На основании раздела V Положения о Территориальном фонде обязательного медицинского страхования Саратовской области, утвержденного постановлением Правительства Саратовской области от 29.03.2011 № 160-П, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в целях обеспечения безопасности конфиденциальной информации, п р и к а з ы в а ю:

1. Утвердить Требования по подключению информационных систем участников системы обязательного медицинского страхования к информационной системе персональных данных и удостоверяющему центру корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области (далее - Требования) согласно приложению к настоящему приказу.
2. Управлению информационных технологий обеспечить размещение настоящих Требований на официальном сайте ТФОМС Саратовской области www.sartfoms.ru.
3. Организационному отделу управления правового и организационного обеспечения довести настоящий приказ до сведения ответственных исполнителей.
4. Контроль за исполнением настоящего приказа возложить на первого заместителя директора.

Директор **А.Н. Саухин**

Приложение

УТВЕРЖДЕНЫ
приказом ТФОМС
Саратовской области
от «16» апреля 2018 г. №74

ТРЕБОВАНИЯ
по подключению информационных систем участников системы обязательного медицинского страхования к информационной системе персональных данных и удостоверяющему центру корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области

Настоящие Требования по подключению информационных систем участников системы обязательного медицинского страхования к информационной системе персональных данных и удостоверяющему центру корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области (далее – Требования) определяют требования и условия, а также устанавливают порядок подключения внешних информационных систем к информационной системе персональных данных (ИСПДн) и удостоверяющему центру корпоративного уровня (УЦКУ) Территориального фонда обязательного медицинского страхования Саратовской области (далее по тексту – ИСПДн, УЦКУ ТФОМС Саратовской области).

Настоящие Требования распространяются на объекты информатизации из состава внешних информационных систем, подключаемых (имеющих подключение) к ИСПДн и УЦКУ ТФОМС Саратовской области.

1. Общие сведения

1.1. ИСПДн ТФОМС Саратовской области создана в соответствии с положениями Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» и постановления Правительства Саратовской области от 29.03.2011 № 160-П «Об утверждении Положения о Территориальном фонде обязательного медицинского страхования Саратовской области».

1.2. В соответствии со статьей 13 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ИСПДн ТФОМС Саратовской области присвоен статус информационной системы «государственная», так как государственные информационные системы - это федеральные информационные системы и региональные информационные системы, созданные на основании, соответственно,

федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

1.3. ТФОМС Саратовской области является владельцем и администратором защищенной сети ViPNet № 602.

1.4. ТФОМС Саратовской области является УЦКУ, обеспечивающим функционирование корпоративной защищенной сети ViPNet № 602 в системе обязательного медицинского страхования Саратовской области.

1.5. Общий порядок и условия предоставления удостоверяющим центром участникам защищенной сети возможность участвовать в обмене юридически значимыми электронными документами с применением электронной подписи и взаимодействия информационных систем устанавливается утвержденным Регламентом УЦКУ ТФОМС Саратовской области.

1.6. ТФОМС Саратовской области является зарегистрированным оператором обработки персональных данных при реализации полномочий и функций ТФОМС Саратовской области в системе обязательного медицинского страхования в соответствии с законодательством Российской Федерации и обеспечивает в пределах своей компетенции защиту сведений, составляющих информацию ограниченного доступа.

1.7. В соответствии с Общими принципами построения и функционирования информационных систем и порядком информационного взаимодействия в сфере обязательного медицинского страхования (утв. приказом Федерального фонда обязательного медицинского страхования от 07.04.2011 № 79) в структуру региональной информационной системы обязательного медицинского страхования, как подсистема, входят:

- информационная система территориального фонда обязательного медицинского страхования;
- информационная система страховой медицинской организации;
- информационная система медицинской организации.

1.8. Все участники информационного взаимодействия в региональной информационной системе обязательного медицинского страхования обязаны обеспечить исполнение законодательства Российской Федерации по вопросам защиты информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

1.9. ИСПДн, УЦКУ ТФОМС Саратовской области имеет аттестат соответствия требованиям информационной безопасности, выданный Органом по аттестации объектов информатизации по требованиям безопасности информации.

1.10. Настоящие Требования публикуются на официальном сайте ТФОМС Саратовской области в сети «Интернет» (www.sartfoms.ru) и обязательны к применению участниками информационного взаимодействия при подключении к ИСПДн, УЦКУ ТФОМС Саратовской области.

2. Основные положения

2.1. Общее описание информационного обмена.

Информационный обмен осуществляется в электронном виде по выделенным или открытым каналам связи, включая сеть Интернет, с использованием средств криптографической защиты информации и электронной подписи в соответствии с требованиями законодательства Российской Федерации в сфере защиты информации и персональных данных гражданина.

2.2. Общие требования по защите информации.

Меры по обеспечению безопасности персональных данных принимаются 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.

Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора, в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Меры по обеспечению безопасности персональных данных реализуются, в том числе, посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка должна проводиться не реже одного раза в 3 года.

3. Технические требования

3.1. Требования к организации подключения.

Организация подключения внешних информационных систем к ИСПДн ТФОМС Саратовской области должна осуществляться в соответствии с:

- требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;

- требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (ФСТЭК России, ФСБ России);

- настоящими Требованиями.

До начала выполнения работ по подключению внешних информационных систем к ИСПДн Саратовской области схема защищенного взаимодействия должна быть согласована с ТФОМС Саратовской области.

3.2. Требования к реализации защищенного взаимодействия.

3.2.1. Общие требования.

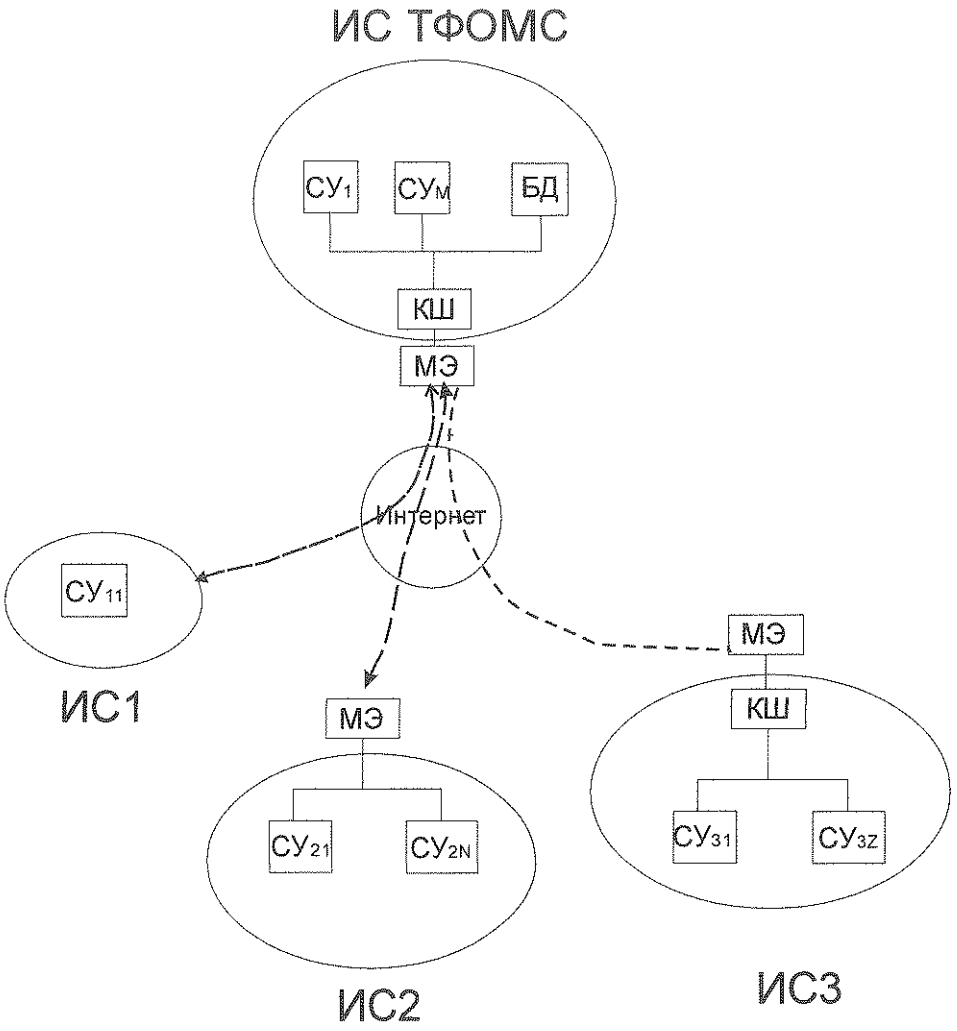
Для организации защищенного взаимодействия внешних информационных систем с ИСПДн Саратовской области во внешних информационных системах должны быть выполнены организационные и технические мероприятия, подтверждающие соответствие системы защиты информации внешних информационных систем требованиям безопасности информации.

Для обеспечения защиты информации во внешних информационных системах должны применяться средства защиты информации, прошедшие процедуру оценки соответствия требованиям по безопасности информации.

Для организации защищенного электронного взаимодействия и информационного обмена между ИСПДн ТФОМС Саратовской области и внешними информационными системами по сети Интернет в состав системы защиты информации внешних информационных систем должны входить шифровальные (криптографические) средства, совместимые с решениями семейства ViPNet.

Для проведения работ по защите информации в ходе создания и эксплуатации внешних информационных систем в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие необходимые для этого лицензии ФСТЭК и/или ФСБ России.

3.2.2. Обобщенная схема подключения внешних информационных систем к ИСПДн ТФОМС Саратовской области.



где:

ИС – информационная система
МЭ – межсетевой экран
КШ – криптошлюз
СУ – сетевой узел

Используется два типа подключения внешних информационных систем к ИСПДн ТФОМС Саратовской области при реализации схемы защищенного взаимодействия.

3.2.3. Требования к реализации схемы защищенного взаимодействия тип № 1.

Взаимодействие внешней информационной системы с ИСПДн ТФОМС Саратовской области должно осуществляться с использованием средства криптографической защиты информации семейства ViPNet, входящего в состав ViPNet сети № 602, владельцем которой является ТФОМС Саратовской области.

Общий порядок и условия подключения к защищенной сети ViPNet № 602 устанавливаются утвержденным Регламентом УЦКУ ТФОМС Саратовской области (далее – Регламент).

Организация защищенного обмена электронными документами и взаимодействие информационных систем в рамках защищенной сети ViPNet № 602 между ТФОМС Саратовской области и подключаемыми организациями производится путем заключения Соглашения о присоединении к Регламенту.

Возможны два варианта реализации схемы защищенного взаимодействия тип № 1.

Схема защищенного взаимодействия тип № 1 (вариант 1).

Для подключения к ИСПДн ТФОМС Саратовской области во внешней информационной системе используется автономное автоматизированное рабочее место (далее – АРМ).

АРМ должен быть оснащен:

- клиентской частью ViPNet - совместимого решения, выполняющего функции средства криптографической защиты информации (сертифицированного ФСБ России);

- сертифицированным средством антивирусной защиты;

- другими сертифицированными средствами защиты информации, необходимыми для нейтрализации актуальных угроз безопасности персональных данных при их обработке при взаимодействии с ИСПДн ТФОМС Саратовской области (при необходимости).

Схема защищенного взаимодействия № 1 (вариант 2).

Для подключения к ИСПДн ТФОМС Саратовской области во внешней информационной системе используются автоматизированные рабочие места в составе локальной вычислительной сети (далее – ЛВС).

На границе ЛВС внешней информационной системы должно быть установлено сертифицированное ФСТЭК/ФСБ России средство межсетевого экранирования.

АРМы должны быть оснащены:

- клиентской частью ViPNet - совместимого решения, выполняющего функции средства криптографической защиты информации (сертифицированного ФСБ России);

- сертифицированным средством антивирусной защиты;

- сертифицированным ФСТЭК России по требованиям безопасности информации средством защиты от несанкционированного доступа.

3.2.4. Требования к реализации схемы защищенного взаимодействия тип № 2.

Схема защищенного взаимодействия тип № 2.

Взаимодействие внешней информационной системы с ИСПДн ТФОМС Саратовской области должно осуществляться с использованием средства криптографической защиты информации семейства ViPNet, входящего в состав ViPNet сети № 602, владельцем которой является ТФОМС Саратовской области, и средства криптографической защиты информации семейства ViPNet, входящего в состав ViPNet сети внешней информационной системы.

Общий порядок и условия подключения к защищенной сети ViPNet № 602 устанавливаются утвержденным Регламентом.

Организация защищенного обмена электронными документами и взаимодействие информационных систем в рамках защищенной сети ViPNet № 602 между ТФОМС Саратовской области и подключаемыми организациями производится путем заключения Соглашения о присоединении к Регламенту, заключения Соглашения об организации информационного взаимодействия и подписания протокола установления межсетевого взаимодействия.

Защищенное взаимодействие осуществляется между сетями ViPNet внешней информационной системы и ИСПДн ТФОМС Саратовской области путем установления межсетевого взаимодействия.

Для подключения к ИСПДн ТФОМС Саратовской области во внешней информационной системе используются автоматизированные рабочие места в составе ЛВС.

На границе ЛВС внешней информационной системы должно быть установлено сертифицированное ФСТЭК/ФСБ России средство межсетевого экранирования.

АРМы должны быть оснащены:

- клиентской частью ViPNet - совместимого решения, выполняющего функции средства криптографической защиты информации (сертифицированного ФСБ России);
- сертифицированным средством антивирусной защиты;
- сертифицированным ФСТЭК России по требованиям безопасности информации средством защиты от несанкционированного доступа.

Данные для передачи в ИСПДн ТФОМС Саратовской области формируются в внешней информационной системе и передаются в ИСПДн ТФОМС Саратовской области через защищенный сертифицированным средством криптографической защиты канал (криптошлюз), образуемый между ViPNet-совместимым решением внешней информационной системе и ViPNet-совместимым решением ТФОМС Саратовской области.

3.2.5. Специальные требования.

Помещения для размещения технических средств и средств защиты информации внешних информационных систем должны удовлетворять требованиям технических условий и эксплуатационной документации на данные средства.

Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ должны выполняться в соответствии с требованиями эксплуатационной документации на данные средства.

Эксплуатация средств защиты информации и СКЗИ должна осуществляться в соответствии с организационно-технической, организационно-распорядительной и эксплуатационной документацией на систему защиты информации внешних информационных систем.

Обеспечение защиты информации в ходе эксплуатации внешних информационных систем осуществляется её владельцем в соответствии с организационно-технической, организационно-распорядительной и эксплуатационной документацией на систему защиты информации внешних

информационных систем и нормативно-техническими документами Российской Федерации в сфере защиты информации.

Для организации взаимодействия внешней информационной системы с ИСПДн ТФОМС Саратовской области подключаемая внешняя информационная система должна иметь комплект документов, подтверждающих соответствие системы защиты информации требованиям безопасности информации.

4. Контроль реализации подключения

4.1. Ответственность за соблюдение настоящих Требований, обеспечение защиты информации, а также ответственность за соблюдение требований к эксплуатации средств защиты информации и СКЗИ в составе системы защиты информации внешних информационных систем, используемых в выбранной схеме подключения, лежит на владельцах подключаемых внешних информационных систем.

4.2. ТФОМС Саратовской области в соответствии с пунктом 7 части 2 статьи 7 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» и положениями приказа Федерального фонда обязательного медицинского страхования от 16.04.2012 № 73 «Об утверждении Положений о контроле за деятельностью страховых медицинских организаций и медицинских организаций в сфере обязательного медицинского страхования территориальными фондами обязательного медицинского страхования» осуществляет контроль за функционированием информационных систем и порядком информационного взаимодействия в сфере обязательного медицинского страхования в пределах предоставленных полномочий.

4.3. В случае выявления нарушений настоящих Требований, ТФОМС Саратовской области имеет право произвести отключение соответствующей информационной системы Участника системы ОМС от ИСПДн ТФОМС Саратовской области (сеть ViPNet № 602).

5. Перечень нормативно-правовых актов

Настоящие Требования разработаны на основании следующих нормативных правовых актов и иных документов:

- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

- приказ Министерства здравоохранения и социального развития Российской Федерации от 28.02.2011 № 158н «Об утверждении Правил обязательного медицинского страхования»;

- приказ Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 № 29н «Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования»;

- приказ Федерального фонда обязательного медицинского страхования от 07.04.2011 № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования»;

- приказ Федерального фонда обязательного медицинского страхования от 16.04.2012 № 73 «Об утверждении Положений о контроле за деятельностью страховых медицинских организаций и медицинских организаций в сфере обязательного медицинского страхования территориальными фондами обязательного медицинского страхования»;

- приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации,

необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- приказ ФСБ Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

- приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- приказ ФСБ Российской Федерации от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;

- приказ ФСБ Российской Федерации от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

- другие нормативные правовые акты Российской Федерации, нормативно-техническая (методическая) документация в области обеспечения информационной безопасности и защиты персональных данных.