Соглашение

о защищенном информационном взаимодействии

и конфиденциальности при осуществлении защищённого информационного взаимодействия

г. Липецк « » \_\_\_\_\_\_\_\_\_\_\_2021 г.

Территориальный фонд обязательного медицинского страхования Липецкой области, в лице директора Ражиной Галины Анатольевны, действующего на основании Положения, именуемый в дальнейшем ТФОМС, с одной стороны, и

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

действующий(ая) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемый(ая) в дальнейшем Пользователь, с другой стороны, заключили настоящее Соглашение о нижеследующем:

**1. Общие положения.**

* 1. Термины, применяемые в настоящем Соглашении, означают следующее:

**Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

**Доступ к информации** - возможность получения информации и ее использования.

**Предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

**Распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

**Информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

**Информационная система ведения персонифицированного учета медицинской помощи, оказанной застрахованным лицам в сфере обязательного медицинского страхования, Территориального фонда обязательного медицинского страхования Липецкой области (ИС ВПУМПЗЛ ТФОМС ЛО)** - информационная система, предназначенная для ведения персонифицированного учета сведений о медицинской помощи, оказанной лицам, застрахованным по обязательному медицинскому страхованию на территории Липецкой области, а также лицам, обратившимся за помощью в медицинские организации Липецкой области.

В рамках данного соглашения к конфиденциальной информации относятся персональные данные и данные составляющие в соответствии с законодательством РФ врачебную тайну.

1. **Предмет Соглашения.**
   1. Предметом Соглашения являются взаимоотношения сторон по обмену сведениями, с учетом Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» с учетом требований Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Федерального закона от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
   2. Стороны осуществляют защищенное информационное взаимодействие в целях организации и ведения персонифицированного учета сведений о медицинской помощи в рамках ИС ВПУМПЗЛ ТФОМС ЛО в целях реализации функций системы обязательного медицинского страхования на территории Липецкой области.
   3. Стороны признают, что используемые ими меры и средства защиты информации, указанные в настоящем Соглашении, достаточны для обеспечения: конфиденциальности информации при взаимодействии Сторон в рамках ИС ВПУМПЗЛ ТФОМС ЛО, отсутствия несанкционированных изменений при взаимодействия Сторон в рамках ИС ВПУМПЗЛ ТФОМС ЛО (подтверждение подлинности информации), подтверждение авторства информации (информация исходит от Стороны, ее передавшей).
   4. Стороны при осуществлении защищенного информационного взаимодействия в рамках ИС ВПУМПЗЛ ТФОМС ЛО обязуются руководствоваться следующими принципами:
      1. Строгого соблюдения Сторонами законодательства Российской Федерации, нормативных актов в области защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.
      2. Строгого соблюдения Сторонами настоящего Соглашения при осуществлении защищенного информационного взаимодействия.
      3. Своевременности предоставления информации о нарушениях в работе технических средств, используемых при защищенном информационном взаимодействии.
      4. Обязательности и безупречности исполнения, достигнутых Сторонами договоренностей.
   5. Защищенное информационное взаимодействие в рамках ИС ВПУМПЗЛ ТФОМС ЛО осуществляется с использованием каналов сети Интернет. Защита информационного взаимодействия осуществляется при помощи системы защиты информации VipNet CUSTOM, включающей в себя средства криптографической защиты информации.
2. **Обязанности и ответственность сторон.**
   1. ТФОМС и Пользователь принимают на себя следующие обязательства:
      1. Обеспечить функционирование оборудования, необходимого для защищенного информационного взаимодействия;
      2. Пользователь приобретает за свой счет средства криптографической защиты информации ViPNetClient (производитель ОАО «ИнфоТеКС»), используемые в ТФОМС Липецкой области.
      3. Пользователь оплачивает средства связи и каналы связи, необходимые для работы при осуществлении защищённого информационного взаимодействии.
      4. После получения регистрационных файлов от ОАО «ИнфоТеКС» ТФОМС Липецкой области формирует дистрибутивы ключей для Абонентских пунктов вместе с паролем доступа к нему и передает Пользователю ключевую информацию, используемую для функционирования средств криптографической защиты информации (далее СКЗИ).
      5. ТФОМС имеет право производить замену СКЗИ в случае изменения требований к СКЗИ. О замене средств криптографической защиты информации, ТФОМС обязан уведомить об этом Пользователя не менее чем за 60 дней. При необходимости Пользователь обязан до наступления данного события приобрести требуемые программно-технические средства в соответствии с рекомендациями ТФОМС и ввести их в действие.
      6. При плановой замене ключевой информации ТФОМС также обязан уведомить об этом Пользователя не менее чем за 15 дней. В свою очередь Пользователь обязан в течение, указанного срока предоставить в ТФОМС необходимые материалы и электронные носители для изготовления новой ключевой информации.
      7. При изменении форматов обмена с ИС ВПУМПЗЛ ТФОМС ЛО, ТФОМС ставит в известность об этом Пользователя не менее чем за 30 дней до наступления события.
      8. ТФОМС обязуется обеспечить конфиденциальность информации, передаваемой Пользователем в рамках настоящего Соглашения в строгом соответствии с действующим законодательством Российской Федерации.
   2. Стороны обязуются:
      1. При осуществлении защищенного информационного взаимодействия руководствоваться законодательством Российской Федерации, включая нормативно-правовые акты, регламентирующие использование средств криптографической защиты информации, и настоящим Соглашением.
      2. Содержать в исправном состоянии рабочие станции, участвующие в информационном взаимодействии, принимать организационные меры для предотвращения несанкционированного доступа к данным рабочим станциям, установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены;
      3. Не допускать появления на взаимодействующих рабочих станциях компьютерных вирусов.
      4. Выполнять требования к эксплуатации средств криптографической защиты информации, указанные в эксплуатационной документации на используемые средства криптографической защиты информации.
      5. Предотвращать несанкционированный доступ к информации и (или) передачу ее лицам, не имеющим права на доступ к информации.
      6. Обеспечивать защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.
      7. Допускать к работе со средствами защиты информации только обученных специалистов, перечень которых определяется Сторонами самостоятельно;
      8. Обеспечить правильность функционирования средств защиты информации, в соответствии с эксплуатационной документацией на средства защиты информации.
      9. Осуществлять постоянный контроль за обеспечением уровня защищенности информации.
      10. Передача конфиденциальной информации по информационно-телекоммуникационной сети может осуществляться только с использованием средств защиты информации сети ТФОМС Липецкой области VipNet № 641.
   3. Стороны несут ответственность по соглашению в соответствии с действующим законодательством.
3. **Дополнительные условия.**
   1. Требования к программно-техническому обеспечению и средствам аутентификации, указанные в приложении 1 к настоящему Соглашению, устанавливаются ТФОМС и являются обязательными для Пользователя.
   2. Все разногласия, споры и конфликтные ситуации, возникающие вследствие выполнения настоящего Соглашения, разрешаются с учетом взаимных интересов путем переговоров.
   3. Стороны, заключившие настоящее Соглашение, могут договориться о внесении в него дополнительных условий, которые после согласования в письменном виде и подписания становятся частью Соглашения.
4. **Срок действия настоящего Соглашения и порядок расторжения.**
   1. Соглашение заключено на срок с \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. по \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.
   2. Соглашение считается продленным на следующие 12 месяцев, если не менее чем за 30 календарных дней до истечения срока действия Соглашения ни одна из сторон не заявит в установленном порядке о его расторжении.
   3. Соглашение может быть расторгнуто:

* по инициативе любой из сторон с предупреждением другой стороны в пятнадцатидневный срок;
* по другим основаниям, предусмотренным законодательством.
  1. Соглашение составлено в 2-х экземплярах, каждый из которых является подлинным и имеет одинаковую юридическую силу. Один экземпляр находится в ТФОМС, второй – у Пользователя.
  2. К настоящему Соглашению прилагаются и являются его неотъемлемой частью:

**Приложение 1**. Требования к программно-техническому обеспечению и средствам защиты информации.

**Приложение 2.** Требования к юридическим лицам, осуществляющим электронный документооборот, содержащий персональные данные, с Территориальным фондом ОМС Липецкой области.

1. **Юридические адреса сторон.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Территориальный фонд обязательного медицинского страхования Липецкой области | | | |  |  | | |
| 398059, г. Липецк, ул.М.Горького, д. 2  Телефон: (4742) 25-19-00 | | | |  |  | | |
|  | | | |  |  | | |
| Директор | | | |  |  | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Г.А.Ражина | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |  |
| « » | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | 2021 г. |  | « » | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г. | |
|  | | | |  |  | | |
| М.П. | | | |  | М.П. | | |

**Приложение 1**

к Соглашению от \_\_\_\_.\_\_\_\_\_. 20 № \_\_\_\_\_\_\_\_\_\_\_

# Требования

**к программно-техническому обеспечению и средствам защиты информации.**

1. Программное обеспечение для создания виртуальных защищенных сетей – ViPNet Client версии 4 и выше.

2. Требования к техническим средствам и операционной среде для установки программного обеспечения ViPNet Client:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.

- Объем оперативной памяти — не менее 1 Гбайт.

- Свободное место на жестком диске — не менее 500 Мбайт (рекомендуется 1 Гбайт).

- Сетевой интерфейс (не более 10 IP-адресов на одном сетевом интерфейсе) или модем.

- Операционная система: Windows 8.1 (32/64-разрядная); Windows Server 2012 (64-разрядная); Windows Server 2012 R2 (64-разрядная); Windows 10 (32/64-разрядная); Windows Server 2016 (64-разрядная); Windows Server 2019 (64-разрядная); .Astra Linux SE «Смоленск» 1.4 (x86\_64), ядро 3.16.0-16-generic; Astra Linux SE «Смоленск» 1.5 (x86\_64), ядро 4.2.0-23-generic; Debian 8.7 (x86\_64), ядро 3.16.0-4, среда рабочего стола GNOME 3; Ubuntu 16.04 (x86\_64), ядро 4.4.0-21-generic — 4.4.0-112-generic; Альт Линукс СПТ 7.0 (x86\_64), ядро 3.14.59-std-def-alt1.M70C.5 — 4.4.127-std-def-alt0.M70C.1; Альт Рабочая станция 8 (x86\_64), ядро 4.4.34-std-def-alt0.M80H.1; Альт 8 СП (x86\_64), ядро 4.4.116 -std-def-alt0.M80C.1; ГосЛинукс 6.6 IC4-RTM (x86\_64), ядро 3.10.104-1.el6; ЛОТОС (x86\_64), ядро 3.16.43; РОСА «КОБАЛЬТ» 7.3 (x86\_64), ядро 3.10.0-514.el7.

- Для операционной системы должен быть установлен самый последний накопительный пакет обновлений.

- На компьютере должно быть установлена антивирусная программа, сертифицированная ФСТЭК России и/или ФСБ России.

3. Требования к компьютеру для установки программы ViPNet Client 4U for Linux:

- Процессор — Intel Core Duo или другой схожий по производительности 64-разрядный процессор.

- Объем оперативной памяти — не менее 1 Гбайт.

- Свободное место на жестком диске — не менее 500 Мбайт (рекомендуется 1 Гбайт).

- Операционная система одного из следующих дистрибутивов: Astra Linux Special Edition «Смоленск»; Astra Linux Common Edition 2.12.29 «Орел»; ГосЛинукс IC5; РЕД ОС 7.2; РЕД ОС 7.3; Альт Рабочая станция 8.2; Альт Рабочая станция 8 СП; Альт Рабочая станция 9.1; ЛОТОС (редакция для серверов и рабочих станций); - РОСА «КОБАЛЬТ» (пользовательская редакция); AlterOS 7.5; EMIAS OS 1.0; Ubuntu 18.04.5 LTS; Ubuntu 20.04.2 LTS; Debian 9.13; Debian 10.9; CentOS 7.1; CentOS 7.9; CentOS 8.2; CentOS 8.3; «Эльбрус»; Astra Linux Special Edition «Ленинград».

4. На компьютере должно быть установлено и настроено средство защиты от несанкционированного доступа Dallas Lock 8.0 версии С/К или его аналоги, прошедшие сертификацию по требованиям ФСТЭК России и/или ФСБ России.

5. На компьютере должен быть установлен и настроен аппаратно-программный модуль доверенной загрузки Соболь версии 3.0 или выше или СДЗ Dallas Lock. Для реализации меры УПД.17 при отсутствии возможности обеспечения доверенной загрузки средств вычислительной техники необходимо использовать реализацию компенсирующих мер, а именно: ЗТС.2, ЗТС.3, пароль на BIOS, опечатывание системного блока и контроль за вскрытием технических средств.

6. На компьютере могут быть установлены следующие операционные системы: Windows 8.1 (32/64-разрядная); Windows Server 2012 (64-разрядная); Windows Server 2012 R2 (64-разрядная); Windows 10 (32/64-разрядная); Windows Server 2016 (64-разрядная); Windows Server 2019; Astra Linux Special Edition «Смоленск»; Astra Linux Common Edition 2.12.29 «Орел»; ГосЛинукс IC5; РЕД ОС 7.2; РЕД ОС 7.3; Альт Рабочая станция 8.2; Альт Рабочая станция 8 СП; Альт Рабочая станция 9.1; ЛОТОС (редакция для серверов и рабочих станций); - РОСА «КОБАЛЬТ» (пользовательская редакция); AlterOS 7.5; EMIAS OS 1.0; Ubuntu 18.04.5 LTS; Ubuntu 20.04.2 LTS; Debian 9.13; Debian 10.9; CentOS 7.1; CentOS 7.9; CentOS 8.2; CentOS 8.3; «Эльбрус»; Astra Linux Special Edition «Ленинград».

7. Для работы с ГИС УОМПиЗЛ ТФОМС ЛО Клиентом должно применяться следующее дополнительное программное обеспечение: КриптоПро CSP, Chromium Gost, Яндекс Браузер.

Приложение 2

к Соглашению от \_\_\_\_.\_\_\_\_\_. 20 № \_\_\_\_\_\_\_\_\_\_\_

**Требования**

к юридическим лицам, осуществляющим электронный

документооборот, содержащий персональные данные, с Территориальным

фондом ОМС Липецкой области

**1. Требования по организационному обеспечению безопасности средств криптографической защиты информации.**

1.1 В организации руководством должны быть назначены сотрудники, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ.

1.2 Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством организации, с учетом эксплуатационной документации на средства криптографической защиты информации.

1.3 В организации должны быть созданы условия, обеспечивающие сохранность конфиденциальной информации, доверенной организации ТФОМС соответствии с действующим законодательством.

**2. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены средства криптографической защиты информации.**

2.1 Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее – помещения), должны обеспечивать безопасность информации, средств криптографической защиты информации, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы посторонними лицами.

2.2 Порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации.

2.3 При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п. окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь входные двери, на которые устанавливаются надежные замки.

2.4 Устанавливаемый руководителем организации порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

2.5 Размещение и установка СКЗИ осуществляется в соответствии с требованиями эксплуатационной документации на СКЗИ.

2.6 Системные блоки ЭВМ с установленными СКЗИ должны быть оборудованы средствами контроля их вскрытия.

**3. Требования к сотрудникам, осуществляющим эксплуатацию и установку (инсталляцию) средств криптографической защиты информации.**

3.1 К работе со СКЗИ допускаются решением руководства организации только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

3.2 Уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

3.3 Руководитель организации или лицо, уполномоченное на руководство заявленными видами деятельности, должно иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

**4. Организационные мероприятия, обязательные к выполнению:**

4.1 Определить рабочие места (объекты информатизации), с помощью которых производится информационный обмен с ИС ВПУМПЗЛ ТФОМС ЛО.

4.2 Назначить ответственного за обеспечение безопасности информации на ОИ (администратора безопасности) или дополнить обязанности ответственного за обеспечение безопасности информации (при его наличии).

4.3 Разработать инструкцию администратора информационной безопасности объектов информатизации. Ознакомить администратора безопасности с инструкцией администратора информационной безопасности объектов информатизации.

4.4 Разработать инструкцию ответственного пользователя средств криптографической защиты информации (далее — СКЗИ).

4.5 Определить сотрудника, на которого будут возложены функции ответственного пользователя СКЗИ (рекомендуется возложить данные обязанности на администратора безопасности).

4.6 Ознакомить ответственного пользователя СКЗИ с «Инструкцией ответственного пользователя средств криптографической защиты информации». Определить перечень лиц, допущенных к работе на объекте информатизации.

4.7 Ознакомить сотрудников со следующими организационно-распорядительными документами под роспись:

4.7.1 «Инструкция по организации парольной защиты на объектах информатизации»;

4.7.2 «Инструкция пользователя объектов информатизации»;

4.7.3 «Инструкция пользователя средств криптографической защиты информации, применяемых на объектах информатизации»;

4.7.4 «Инструкция по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации, применяемых на объектах информатизации»;

4.7.5 «Инструкция по регистрации, выявлению инцидентов (событий безопасности) и реагированию на них на объектах информатизации»;

4.7.6 «Инструкция по организации учета, хранения и эксплуатации средств защиты информации, применяемых на объектах»;

4.7.7 «Инструкция по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации, применяемым на объектах информатизации»;

4.7.8 «Инструкция по уничтожению ключевой информации к средствам криптографической защиты информации, применяемым на объектах информатизации».

4.8. Определить сотрудников, ответственных за помещения, в которых расположены объекты информатизации.

4.9 Ознакомить ответственных сотрудников с «Инструкцией об организации безопасности помещений, в которых размещены объекты информатизации».

4.10 Разработать и утвердить следующую эксплуатационную документацию объектов информатизации:

4.10.1 Технический паспорт на ОИ «Типовой АРМ»;

4.10.2 Журнал учета машинных носителей информации ограниченного доступа;

4.10.3 Журнал учета используемых криптосредств, эксплуатационной и технической документации к ним, ключевых документов;

4.10.4 Журнал учета мероприятий по обеспечению контроля состояния защиты информации на объектах информатизации».

4.11 Определить администратора информационной безопасности ОИ ответственным за ведение и поддержание в актуальном состоянии эксплуатационной документации на объектах информатизации».

4.12 Утвердить План мероприятий по обеспечению контроля состояния обеспечения безопасности информации объектов информатизации».

После выполнения перечисленных выше пунктов необходимо предоставить подтверждение проведенных мероприятий в ТФОМС Липецкой области.