Приложение 1 к приказу МЗ РС(Я) от «»_____2020г. №
и ТФОМС РС(Я) от «»_____2020г. №

РЕГЛАМЕНТ

организации электронного юридически значимого документооборота между участниками информационного взаимодействия в сфере обязательного медицинского страхования на территории Республики Саха (Якутия)

1. Общие положения

1.1 Регламент организации электронного юридически значимого документооборота между участниками информационного взаимодействия в сфере обязательного медицинского страхования на территории Республики Саха (Якутия) (далее - Регламент) разработан во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», приказа Минздравсоцразвития России от 25.01.2011 № 29н «Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования», приказа Минздрава России от 28.02.2019 N 108н "Об утверждении Правил обязательного медицинского страхования", приказа ФОМС от 07.04.2011 № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования.

1.2 Регламент определяет правила и порядок организации электронного юридически значимого документооборота между участниками информационного взаимодействия в сфере обязательного медицинского страхования Республики Саха (Якутия) (далее – участники информационного взаимодействия) при обмене информационными документами (электронными документами) по защищенным каналам связи.

2. Основные определения

2.1 Для целей Регламента используются следующие основные понятия:

участники информационного взаимодействия – участники обязательного медицинского страхования на территории Республики Саха (Якутия), осуществляющие обмен информацией в электронной форме;

документ – материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения;

Электронный документ - документ, в котором информация представлена в электронной форме для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Юридическая значимость электронного документа подтверждается Электронной подписью;

юридическая значимость электронного документа – свойство электронного документа, позволяющее воспринимать содержание данного электронного документа как подлинное;

электронная подпись (далее -ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

целостность электронного документа – состояние электронного документа, в который после его создания не вносились никакие изменения;

удостоверяющий центр – юридическое лицо, Федеральный фонд обязательного медицинского страхования осуществляющий функции по созданию и выдаче сертификатов ключей электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

уполномоченная организация удостоверяющего центра электронной подписи автоматизированных информационных систем единого информационного пространства системы обязательного медицинского страхования – Территориальный фонд обязательного медицинского страхования Республики Саха (Якутия), в части предоставления услуг удостоверяющего центра электронной подписи автоматизированных информационных систем единого информационного пространства системы обязательного медицинского страхования;

СКЗИ- (средство криптографической защиты)-аппаратные и (или) программные средства, обеспечивающие применение ЭП (создание, проверка ЭП, создание ключа ЭП и ключа проверки ЭП), и (или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;

владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

3. Принципы и порядок организации информационного взаимодействия

3.1 Под юридически значимым электронным документооборотом понимается обмен электронными документами между участниками информационного взаимодействия, подписанными электронной подписью.

3.2 В качестве средства электронной подписи, обеспечивающего реализацию функций создания электронной подписи в электронном документе с использованием закрытого ключа электронной подписи, подтверждения с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе, создания закрытых и открытых ключей электронных подписей, используется сертифицированные СКЗИ ViPNet и СКЗИ КриптоПро, КриптоАРМ.

3.3 Участники самостоятельно осуществляют приобретение необходимых сертифицированных программных продуктов и носителей для электронных подписей.

Участник допускается к осуществлению электронного документооборота с ТФОМС РС(Я) после выполнения им следующих действий:

– наличие Договора с ТФОМС РС(Я) о финансовом обеспечении обязательного медицинского страхования (для страховой медицинской организации) наличие Договора на предоставление медицинской помощи по ОМС (для медицинских учреждений);

– участник подключен к защищённой сети ОМС;

– назначения лиц, уполномоченных осуществлять обмен ЭД и использовать электронные подписи (пользователей Участника), приказом Участника;

– аттестации рабочего места в соответствии с требованиями, изложенными в Приложении № 1 к настоящему Регламенту;

– формирования ключевой информации в соответствии с Заявкой (Приложение №2), генерации закрытого и открытого ключей ЭП, формирования запроса с последующим получением сертификата ЭП в порядке, установленным настоящим Регламентом;

– установки ПО «ViPNet» на АРМ Участника;

– установки ПО КриптоПРО и КриптоАРМ на АРМ Участника;

- Доверенность на получение ЭП по приложению № 6

3.4 Участники осуществляют передачу и прием юридически значимых электронных документов по телекоммуникационным каналам связи.

3.5 Используемые при информационном взаимодействии участников,

электронные документы с ЭП, сформированные Участниками средствами СКЗИ, имеют равную юридическую силу с документами на бумажном носителе, подписанными соответствующими собственноручными подписями уполномоченных сотрудников участников. При этом для их ЭП соблюдены следующие условия:

сертификаты изданы УЦ (удостоверяющий центр) и не утратили силу (действуют) на момент проверки или на момент подписания электронного документа;

ЭП используется в соответствии со сведениями, указанными в сертификате (Приложение 3).

3.6 Участники признают, что используемые при ЮЗ ЭД в системе СКЗИ, реализующие функции создания ЭП, достаточны для подтверждения следующего:

электронный документ подписан уполномоченным сотрудником стороны его направившей (подтверждение авторства отправленного электронного документа);

электронный документ не претерпел изменений в процессе передачи.

3.7 Электронной подписью подписываются:

− документы между ТФОМС РС (Я), МО и СМО при осуществлении персонифицированного учета оказанной медицинской помощи;

− документы при осуществлении расчетов за медицинскую помощь, оказанную застрахованным лицам за пределами субъекта Российской Федерации, на территории которого выдан полис ОМС;

3.9 Обмен информацией в электронном виде осуществляется с использованием защищенной сети ViPNet.

3.10 Входящий и исходящий электронный документ, подписанный электронной подписью, должен быть зарегистрирован в соответствии с инструкциями по делопроизводству, принятыми в организации.

4 Пользователи Участника

4.1. Пользователями Участника являются только работники Участника, осуществляющие формирование, отправку/получение, проверку, хранение и учет электронных документов и/или обеспечивающие эксплуатацию АРМ Участника, обладающие соответствующей квалификацией.

4.2. Состав пользователей Участника для обмена ЭД, утверждается приказом Участника. В соответствии с выполняемыми должностными обязанностями определены следующие обязательные категории работников, которые имеют допуск к работе в электронной подписью (один пользователь Участника может совмещать несколько категорий):

– администратор АРМ обмена ЭД – работник Участника, отвечающий за организацию и обеспечение бесперебойной эксплуатации программно-технических средств АРМ Участника, за обеспечение и контроль мероприятий по защите информации, за хранение и учет ЭД, за взаимодействие с ТФОМС

РС (Я) по техническим вопросам и вопросам обеспечения безопасности информации;

– уполномоченные - должностные лица и работники Участника, наделенные правом использования ЭП в ЭД.

Сведения о составе пользователей предоставляются в ТФОМС РС (Я) вместе с заверенными копиями соответствующих приказов и все изменения в составе пользователей своевременно доводятся до Фонда по защищенной сети VIPNet на адрес: «АП ТФОМС РС(Я) Герасимов М.М. Оператор УЦ».

4.3. Пользователи Участника несут персональную ответственность за обеспечение безопасного использования ключевой информации, паролей и обязаны обеспечивать ее сохранность, неразглашение и нераспространение в соответствии с действующим законодательством РФ.

4.4. Пользователи Участника, должны быть ознакомлены под роспись с документами, регламентирующими обмен ЭД в ТФОМС РС(Я).

4.5. Пользователи Участника, назначенные приказом обязаны дать подписку о неразглашении предоставленной им информации.

4.6. Администратор АРМ Участника, назначенный приказом, в случае увольнения уполномоченных лиц, обязан сменить пароль для обеспечения защиты информации в ТФОМС РС(Я).

4.7. Пользователи Участника, назначенные приказом Администратором АРМ Участника, в случае их увольнения, обязаны дать подписку о неразглашении предоставленной им информации в ТФОМС РС(Я), сдать ключевую и парольную информацию руководителю Участника, до назначения нового работника, после издания соответствующего приказа.

4.8 Формирование запроса на издание сертификата ЭП осуществляется Участником.

Запрос на издание ЭП в электронном виде Администратору ТФОМС РС(Я).

Заявка на выдачу сертификата ЭП (Приложение №2), оформленная и подписанная в установленном порядке в бумажном виде, направляются Администратору ТФОМС Р(Я) который в срок, не превышающий 5 рабочих дней с момента получения Заявки, издает соответствующие новый сертификат ЭП.

5. Порядок хранения документов

5.1 Участники информационного взаимодействия организуют архивы электронных документов, отправленных (полученных) в рамках Регламента. Сроки хранения электронных документов устанавливаются в соответствии со сроками хранения аналогичных документов на бумажных носителях. Наряду с хранением электронных документов Участники информационного взаимодействия организуют хранение соответствующих журналов учета, сертификатов ключей подписи, уведомлений о доставке документа в течение срока, соответствующего сроку хранения соответствующих электронных документов.

5.2 Обязательными условиями хранения электронных документов

являются:

наличие в архиве организации не менее двух экземпляров каждой единицы хранения электронных документов (подписанный и подписанный рабочий экземпляры должны находиться на разных физических устройствах);

обеспечение режима хранения электронных документов, исключающего утрату, несанкционированную рассылку, уничтожение или искажение информации.

5.3 Передача текстовых электронных документов для хранения в архив организации, являющейся источником комплектования архива, осуществляется в общедоступном формате.

5.4 В случае, если при осуществлении технического контроля установлены изменения физического состояния носителей электронных документов, архив организации по решению руководителя организации должен проводить работу по перезаписи электронных документов на новые носители.

5.6 При изменении форматов в результате преобразования программно-аппаратной среды, ухудшении воспроизводимости электронных документов архив организации по решению руководителя организации должен проводить работу по перезаписи электронных документов в новые форматы.

5.7 При осуществлении перезаписи должна быть обеспечена аутентичность, полнота, достоверность, целостность и неизменность информации, содержащейся в электронных документах.

5.8 Перечень документов, обмен которыми осуществляется в электронном виде, подписывается уполномоченными что и на бумажном экземпляре.

5.9 Учет ключевой информации, содержащейся на материальных носителях информации, осуществляется Администратором Фонда и Участниками путем ведения журналов (Приложения № 4 и № 5 к настоящему Регламенту).

5.10 В случае необходимости замены ключей шифрования и ЭП Участнику необходимо:

- представить в ТФОМС РС (Я) заявку на изготовление ключей шифрования и ЭП;

- в течение 5 рабочих дней после получения новых ключей шифрования и ЭП уничтожить и составить акт уничтожения прежних ключей шифрования (Приложение №7 к Регламенту).

6. Признание электронной подписи

6.1 Электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте

подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания;

квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

При этом проверка осуществляется с использованием квалифицированного сертификата лица, подписавшего электронный документ.

7. Информационная безопасность

7.1 Обмен электронными документами между участниками информационного взаимодействия осуществляется по защищенным каналам связи с использованием технологии ViPNet, в рамках соглашения об информационном взаимодействии между участниками обязательного медицинского страхования Республики Саха (Якутия)

7.2 В случае временного отсутствия у участника информационного взаимодействия технической возможности осуществлять передачу электронных документов по защищенным каналам связи с использованием технологии ViPNet, участник информационного взаимодействия передает электронные документы на машинных носителях (оптический диск, карта памяти, USB накопитель), при этом электронные документы должны быть подписаны электронной подписью.

7.3 Участники информационного взаимодействия при ведении электронного юридически значимого документооборота, хранении электронных архивов обязаны принимать необходимые правовые, организационные и технические меры для защиты конфиденциальной информации, в том числе персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

7.4 Обеспечение сохранности и конфиденциальности электронных документов, защита элементов среды электронного взаимодействия от несанкционированного доступа, компьютерных атак и воздействий вредоносного программного обеспечения в целом обеспечивается применением следующих мер защиты:

использованием средств антивирусной защиты и систем защиты от воздействия вредоносного кода в точках соединения систем обработки, хранения и передачи сообщений (документов) с публичными сетями, контролем подозрительных активностей в информационной системе;

контролем целостности передаваемых юридически значимых электронных документов, квитанций, подтверждений и т.д.;

использованием средств защиты от несанкционированного доступа на оборудовании;

реализацией систем управления доступом к электронным документам на базе метаданных электронного документа и использованием систем аутентификации субъектов доступа;

обеспечением аутентичности электронных документов и их метаданных на всем сроке хранения;

контролем целостности информации.

7.5 Использование, учет, распространение и техническое обслуживание средств криптографической защиты информации осуществляется в соответствии с требованиями законодательства Российской Федерации и иными нормативными правовыми актами.

7.6 При использовании электронных подписей участники информационного взаимодействия обязаны:

обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

уведомлять Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников информационного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с законодательством Российской Федерации.

7.7 Проверку соблюдения участниками информационного взаимодействия требований законодательства Российской Федерации в области защиты информации при организации и осуществлении информационного взаимодействия в рамках Регламента на территории Республики Саха (Якутия), осуществляет ТФОМС Республики Саха (Якутия).

8. Разрешение конфликтных ситуаций

8.1 В связи с осуществлением информационного взаимодействия возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной подписи. Данные конфликтные ситуации могут возникать в частности, в следующих случаях:

неподтверждение подлинности электронных документов средствами электронной подписи участника информационного взаимодействия, получившего электронный документ;

оспаривание факта формирования электронного документа;

оспаривание факта идентификации владельца сертификата ключа электронной подписи, подписавшего документ;

заявление участника информационного взаимодействия об искажении электронного документа;

оспаривание факта отправления и/или доставки электронного документа;

оспаривание аутентичности экземпляров электронных документов;

иные случаи возникновения конфликтных ситуаций, связанных с осуществлением информационного взаимодействия.

8.2 Конфликтная ситуация возникает также в случае, если участник информационного взаимодействия высказывает недоверие к программному обеспечению, функционирующему на рабочем месте другого участника информационного взаимодействия.

8.3 В случае возникновения конфликтной ситуации участник информационного взаимодействия, предполагающий возникновение конфликтной ситуации, должен незамедлительно, но не позднее чем в течение одного рабочего дня после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации участнику информационного взаимодействия, являющемуся другой стороной конфликта, а также в ТФОМС Республики Саха (Якутия).

8.4 Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, свидетельствуют о наличии конфликтной ситуации. Кроме того, в нем должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

8.5 Подтверждение подлинности электронной подписи в электронном документе производится в соответствии с Регламентом предоставления услуг Уполномоченной организацией - ТФОМС РС(Я), Удостоверяющего центра электронной подписи автоматизированных информационных систем единого информационного пространства системы обязательного медицинского страхования.

8.6 Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если участник информационного взаимодействия удовлетворен информацией, полученной от других участников информационного взаимодействия, которым было направлено уведомление и при отсутствии возражений ТФОМС Республики Саха (Якутия). В противном случае, для разрешения конфликтной ситуации ТФОМС Республики Саха (Якутия) формирует комиссию.

8.7 Если участники информационного взаимодействия, являющиеся сторонами в конфликтной ситуации, не договорятся об ином, в состав комиссии включается равное количество представителей конфликтующих сторон.

8.8 При необходимости к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты.

8.9 Сформированная комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, являющихся причиной возникновения конфликтной ситуации.

8.10 Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.

8.11 По итогам работы составляется акт, в котором содержится изложение выводов комиссии по существу вопросов и причин возникновения конфликтной ситуации. Помимо этого, акт должен также содержать следующие данные:

Рекомендуемый состав комиссии:

Руководитель, 1 заместитель, юрист, экономист, администратор УЦ, IT сотрудник;

дату и место составления акта;

даты и время начала и окончания работы комиссии;

перечень мероприятий, проведенных комиссией;

подписи членов комиссии;

указание на особое мнение члена (или членов) комиссии, в случае наличия такового.

8.12 Выводы комиссии могут быть использованы участниками информационного взаимодействия при урегулировании конфликта в досудебном порядке.

8.13 Участники информационного взаимодействия обязаны принимать все возможные усилия для разрешения споров путем переговоров. Если в результате переговоров участники информационного взаимодействия не придут к согласию, спор рассматривается в судебном порядке.

9. Приложения к Регламенту

9.1. Приложение №1 - Акт аттестации рабочего места для работы в ИСПД ТФОМС РС(Я).

9.2. Приложение №2 - Заявка на изготовление ключей шифрования и ЭП, на получение сертификата ключа электронной цифровой подписи.

9.3. Приложение №3 - Сертификат ключа подписи

9.4. Приложение №4 - Журнал учета ключевых документов (ведется Участником).

9.5. Приложение №5 - Журнал учета ключевых документов (ведется ТФОМС РС(Я)).

9.6. Приложение №6 - Доверенность.

9.7. Приложение №7 - Акт уничтожения ключевых документов.

Приложение № 1

Акт аттестации

рабочего места в ТФОМС РС(Я)

Комиссия в составе председателя:

_____

(должность, Ф.И.О.)

и членов комиссии:

_____

(должность, Ф.И.О.)

_____

(должность, Ф. И.О.)

составили настоящий Акт в том, что в кабинете №_____, на рабочей станции (системный блок №_____), проведены работы по оборудованию автоматизированного рабочего места системы электронного документооборота в ТФОМС РС(Я) (клиента VIPNet, КриптоПро, КриптоАРМ).

Работы по оборудованию автоматизированного рабочего места системы электронного документооборота в ТФОМС РС(Я) (клиента VIPNet проведены в соответствии с требованиями 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, утвержденной приказом ФАПСИ от 13.06.2001 г. № 152, а также требованиями технической и эксплуатационной документации.

Примечание:

1.Требования к компьютеру для подключения к ИСПД ТФОМС РС(Я)

Программное обеспечение «ViPNet Клиент», КриптоПро и КриптоАРМ должны эксплуатироваться на персональных компьютерах, ноутбуках, виртуальных машинах, удовлетворяющих следующей конфигурации:

Процессор	Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более
Оперативная память	не менее 512 Мбайт
Свободное место на жестком диске	не менее 150 Мбайт, для дальнейшей работы и хранения архивов и почтовых сообщений рекомендуется не менее 3 Гбайт
Операционная система	Server 2003 (32/64-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7,8,10 (32/64-разрядная), Server 2008 R2, Server 2012 R2 На компьютере должен быть установлен накопительный

	пакет обновления часовых поясов KB2570791.
Дополнительно	На компьютере не должно быть установлено никаких других персональных сетевых экранов (Firewall).
	Доступ к Интернет.

2.Требования к помещению для подключения к ТФОМС РС(Я)

Для обеспечения информационной безопасности необходимо ограничить доступ посторонних лиц в помещение с компьютером, подключенным к ТФОМС РС (Я).

В отсутствие ответственного лица помещение должно закрываться на ключ, электронный идентификатор должен находится у ответственного лица.

Председатель Комиссии _____ (подпись) /_____ (Ф.И.О.)

Члены комиссии: _____ (подпись) /_____ (Ф.И.О.)

_____ (подпись) /_____ (Ф.И.О.)

_____ (подпись) /_____ (Ф.И.О.)

Ответственный за эксплуатацию АРМ _____ (подпись) /_____ (Ф.И.О.)

Участник:

Руководитель

_____/_____/
(подпись) (Ф.И.О.)

м.п.

«_____» _____20__

Приложение № 2

Директору
ТФОМС РС(Я)
А.В. Горохову

Заявка

на получение сертификата ключа электронной подписи

В связи с _____
(предоставлением права использования ЭП, плановой сменой, изменением реквизитов владельца или указать другую причину)

прошу изготовить необходимые для работы электронные подписи(ЭП) и выдать сертификат ключа ЭП Участнику:

Полное наименование организации:

_____

_____

Краткое наименование организации:_____

Телефон: (код города)_____ Факс: _____

e-mail: _____

Ф.И.О. (владельца сертификата ключа подписи): _____

Паспорт: серия_____ № _____ дата выдачи _____ Кем выдан: _____

Должность: _____

Подразделение: _____

В соответствии со ст.9 Федерального закона Российской Федерации от 27.07.2006г. № 152-ФЗ «О персональных данных» я даю согласие на обработку в Удостоверяющем центре ТФОМС РС(Я) своих персональных данных, указанных в настоящем заявлении, а так же в других документах, в целях идентификации и аутентификации меня в качестве Пользователя. Я согласен с тем, что перечень действий, общее описание способов обработки персональных данных, срок обработки, а также условия отзыва данного согласия, установлены Регламентом ТФОМС РС(Я)

Согласен, что мои персональные данные, вносимые в сертификаты, владельцем которых я буду являться, относятся к общедоступным персональным данным.

К заявлению прилагаю: (копии заверяются подписью уполномоченного лица и печатью организации):

1. Копию паспорта Пользователя (страница с Ф.И.О. и фото);
2. Копию свидетельства о постановке на учет в налоговом органе физического лица Пользователя ;

3. Копию страхового свидетельства обязательного пенсионного страхования Пользователя ;

4. Копию свидетельства о государственной регистрации юридического лица или свидетельства о внесении записи в ЕГРЮЛ о юридическом лице, зарегистрированном до 1 июля 2002 года;

5. Копию свидетельства о постановке на учет юридического лица в налоговом органе;

6. Копию документа о назначении на должность от _____ № _____;

Наименование средств, с которыми используется открытый ключ электронной подписи:

- СКЗИ **ViPNet;**
- КриптоПРО
- КриптоАРМ
- Сертификат предназначен для **ТФОМС РС(Я).**

Пользователь _____/_____

(подпись) (Ф.И.О.)

Руководитель _____/_____

(подпись) (Ф.И.О.)

М.П.

«_____» _____20____г.

Приложение №3

Удостоверяющий центр ТФОМС РС(Я)

Удостоверяющий центр электронной подписи автоматизированных информационных систем единого информационного пространства системы обязательного медицинского страхования копия сертификата ключа проверки электронной подписи

Сведения о сертификате:

Версия: 3
Серийный номер: 0097B8752Б16АСС080Е711Р4БВ8СЕЕ5068
Издатель сертификата: CN=УЦ системы ОМС, 0=Федеральный фонд ОМС, STREET=Новослободская ул., д.37, L=Москва, S=Москва, C=RU
Владелец сертификата: **CN**=ТФОМС Республики Саха (Якутия), OU=СМЭБ, O=ТФОМС Республики Саха (Якутия), STREET=ул. Кирова 21 "Б", L=Якутск, S=Республика Саха (Якутия), C=RU

Срок действия:
Действителен с: 00.00.2000 00:00:00
Действителен по: 00.00.2000 00:00:00

Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Значение: 0000 0000 0000 0000 0000 0000 0000 00000

Расширения сертификата X.509
Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)

Расширение: Идентификатор ключа субъекта
Идентификатор: 2.5.29.14
Значение: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Расширение: Сведения о шаблоне сертификата
Идентификатор: 1.3.6.1.4.1.311.21.7
Значение: Шаблон=1.2.643.2.2.50.1.9.00000.00000.00000.00000.00000.00000, Основная версия=1, Вспомогательная версия=0

Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00, Поставщик сертификата: Адрес каталога:CN=УЦ 1 ИС ГУЦ, C=RU, S=77 г. Москва, L=Москва, O=Минкомсвязь России, STREET=125375 г. Москва ул. Тверская д.7, Серийный номер сертификата=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Расширение: Улучшенный ключ
Идентификатор: 2.5.29.37
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4), Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

Расширение: Политики применения
Идентификатор: 1.3.6.1.4.1.311.21.10
Значение: [1]Политика сертификата приложения: Идентификатор политики=Проверка подлинности клиента, [2]Политика сертификата приложения: Идентификатор политики=Защищенная электронная почта, [3]Политика сертификата приложения: Идентификатор политики=Проверка подлинности сервера

Расширение: Политики сертификата
Идентификатор: 2.5.29.32
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата: Идентификатор политики=Класс средства ЭП КС2

Расширение: Средства электронной подписи и УЦ издателя

Идентификатор: 1.2.643.100.112

Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0) (заключение: Сертификат соответствия № СФ/124-2864 от 20.03.2016), средство удостоверяющего центра: ПАК "Удостоверяющий центр "КриптоПро УЦ" версии 2.0 (заключение: Сертификат соответствия № СФ/128-2983 от 18.11.2016)

Расширение: Средство электронной подписи владельца

Идентификатор: 1.2.643.100.111

Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP"

Расширение: Точки распространения списков отзыва (СКЬ)

Идентификатор: 2.5.29.31

Значение: [1]Точка распределения списка отзыва (СКЬ): Имя точки распространения: Полное имя:URL=http://ucfoms.ffoms.ru/cdp/000000000000000.crt

Расширение: Доступ к информации о центрах сертификации

Идентификатор: 1.3.6.1.5.5.7.1.1

Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное
имя= URL=http://ucfoms.ffoms.ru/aia/000000000000000.crt

Расширение: Период использования ключа электронной подписи

Идентификатор: 2.5.29.16

Значение: Действителен с 00.00.2000 г. 00:00:00 по 00.2000 г. 00:00:00

Подпись Удостоверяющего центра:

Алгоритм подписи: ГОСТ Р 34.11/34.10-2001 (1.2.643.2.2.3)

Параметры:

Значение: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Подпись владельца сертификата: _____/_____

"_____" _____20_ г.

Подпись уполномоченного лица УЦ ЭП ФОМС: _____/_____

"_____" _____20_ г.

М. П.

Приложение № 4

Журнал

учета ключевых документов

(ведется Участником)

№№ п/п	внутренний учетный номер	тип ключевого носителя	отметка о получении					отметка об уничтожении ключевой информации		примечания
			№ ключевого носителя	откуда поступил, № и дата сопроводительного письма (акта)	ФИО ответственного за хранение	подпись	дата	дата уничтожения	подпись	
1	2	4	5	6	7	8	9	10	11	12

Все листы в журнале должны быть пронумерованы. Журнал должны быть прошнурован, опечатан и заверен подписью руководителя и печатью организации.

Приложение № 5

Журнал

учета ключевых документов

(ведется ТФОМС РС(Я))

№ п/п	тип ключевого носителя	экз №	отметка об изготовлении			отметка о передаче				примечание
			ф.и.о. изготовившего кд	подпись изготови-вшего кд	дата изготов-ления	наименование участника	Ф.И.О. получателя кд	подпись получателя кд	дата передачи кд	
1	2	3	4	5	6	7	8	9	10	11

Все листы в журнале должны быть пронумерованы. Журнал должны быть прошнурован, опечатан и заверен подписью руководителя и печатью организации.

Приложение № 6

_

ДОВЕРЕННОСТЬ

на выполнение действий от лица сотрудника организации

« » 20 г.

(наименование населенного пункта)

Настоящей доверенностью я,

(должность, Ф.И.О.)

(должность, Ф.И.О.)

паспорт серия № выдан

(кем и когда выдан)

(кем и когда выдан)

уполномочиваю

(должность, Ф.И.О. уполномоченного лица)

паспорт серия № выдан

(кем и когда выдан)

(кем и когда выдан)

совершать следующие действия:

1. Передавать в Удостоверяющий центр Территориального фонда обязательного медицинского страхования Республики Саха (Якутия) (далее-ТФОМС РС(Я)) комплект документов, предусмотренных Регламентом ТФОМС РС(Я), для регистрации, создания сертификата ключа проверки электронной подписи;

2. Получать в Удостоверяющем центре ТФОМС РС(Я) сертификат ключа проверки электронной подписи в электронном виде и на бумажном носителе;

3. Ознакомиться с информацией, содержащейся в заявлениях, запросах на изготовление, аннулирование (отзыв), приостановку сертификатов и

информацией содержащейся в получаемых сертификатах ключей проверки электронных подписей включая кодовые, парольные фразы;

4. Получать в Удостоверяющем центре ТФОМС РС(Я) средства криптографической защиты информации, средства электронной подписи;

5. Передавать в Удостоверяющий центр ТФОМС РС(Я) заявления на аннулирование сертификатов ключей подписей;

7. Расписываться в соответствующих учетных формах, предназначенных для исполнения поручений определенных настоящей доверенностью в том числе, сертификате ключа проверки электронной подписи.

Настоящая доверенность выдана по «____»_____20____г. без права передоверия.

Подпись уполномоченного лица _____ _____ удостоверяю.
(подпись) (Ф.И.О.)

_____ _____ _____
(должность доверителя) (подпись) (Ф.И.О.)

_____ _____ _____
(должность руководителя) (подпись) (Ф.И.О.)

«___»_____20__г.

М.П.

Приложение № 7

0

АКТ

уничтожения ключевых документов

№ _____

г._____ «____» _____ 20_ __ г

Комиссия, в соответствии с приказом _____

(наименование юридического лица участника)

№_____ от «____» _____ 20_ __ г

в составе: председателя _____ , и членов: _____, _____, _____.в связи с _____ подготовила к уничтожению ключевые документы, указанные в табл. 1, путем стирания ключевой информации.

Таблица 1.

тип ключевого носителя	учетный №	экз. №	серийный номер сертификата ключа

При проверке носителя информации установлено, что информация с носителей, указанных в табл. 2, не может быть удалена, и носители подлежат физическому уничтожению.

Таблица 2.

тип ключевого носителя	учетный №	экз. №	серийный номер сертификата ключа
	---	---	---
	---	---	---

(подпись) (Ф.И.О.)

(подпись) (Ф.И.О.)

(подпись) (Ф.И.О.)

РАЗРЕШАЮ УНИЧТОЖИТЬ

_____
(руководитель организации)

_____
(подпись)(Ф.И.О.)

МП «_____» _____ 20_ __ г.

Ключевые документы, перечисленные в табл. 1, уничтожены стиранием ключевой информации двойным форматированием.

Ключевые документы, перечисленные в табл. 2, уничтожены методом разрушения носителя.

Всего уничтожено_____ ( ) ключевых документов

_____ (подпись)	_____ (Ф.И.О.)
_____ (подпись)	_____ (Ф.И.О.)
_____ (подпись)	_____ (Ф.И.О.)
_____ (подпись)	_____ (Ф.И.О.)

Отметки об уничтожении ключевых документов в журнале поэкземплярного учета ключевых документов произвел

_____/_____/_____

должность Ф.И.О. подпись

Акт составлен в 2-х экземплярах:

1-й экземпляр – в дело

2-й экземпляр – администратору ТФОМС РС(Я).