УТВЕРЖДАЮ
Директор Хабаровского краевого
фонда обязательного медицинского
страхования

Е.В. Пузакова

«14» февраля 2020 г.

РЕГЛАМЕНТ
технического и информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и понятия, используемые в настоящем Соглашении, применяются в значениях, установленных действующим законодательством Российской Федерации, эксплуатационной документацией на ПК ViPNet.

ПО – программное обеспечение.
ЦУС – центр управлению сетью ViPNet
ЭД – электронный документ
АРМ – автоматизированное рабочее место
ОМС – обязательное медицинское страхование
СКЗИ – средство криптографической защиты информации.

ХКФОМС – Хабаровский краевой фонд обязательного медицинского страхования.

Регламент – Регламент технического и информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования.

Ресурсы ХКФОМС – совокупность сведений, содержащихся в базах данных, а также информационных технологий и технических средств, обеспечивающих обработку информации.

Участник – организация, признающая данный Регламент.

Пользователь – физическое лицо Участника.

Администратор – уполномоченное лицо, назначенное Участником для обеспечения информационной безопасности в организации.

Уполномоченный работник - лицо, которое действует по доверенности или на основании распорядительного документа.

Средства криптографической защиты информации – программные средства, реализующие алгоритмы криптографического преобразования информации и предназначенные для обеспечения ее конфиденциальности и (или) целостности.

Центр управления сетью – ПО предназначенное для создания и управления конфигурацией виртуальной сети на базе распределенной системы персональных и межсетевых экранов Технологии ViPNet, обеспечивающей защиту функционирования компьютеров и передаваемой информации в защищенной сети.

Плановая смена ключей – смена ключей с установленной периодичностью, не вызванная Компрометацией ключей.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Регламент определяет правила и порядок организации информационных систем Участников информационного взаимодействия в сфере обязательного медицинского страхования Хабаровского края при обмене информационными сообщениями по защищенным каналам связи.

Регламент устанавливает обязательные требования к составу и содержанию организационных и технических мер по обеспечению безопасности информации при ее обработке в информационных системах Участников технического и информационного взаимодействия.

Настоящее Соглашение определяет условия и порядок организации межсетевого взаимодействия между развернутыми у каждой из Участников защищенными виртуальными частными сетями, построенными с использованием программного комплекса ViPNet.

Сформулированные в рамках Регламента требования, принципы и правила являются обязательными для всех Участников технического и информационного взаимодействия.

Регламент разработан во исполнение следующих нормативных актов:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 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 ФОМС от 07.04.2011 № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования».

3. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ

Участник имеет право:

- обратиться в ХКФОМС для регистрации Пользователя;
- обратиться в ХКФОМС для удаления Пользователя;
- обратиться в ХКФОМС для приостановления информационного взаимодействия;
- обратиться в ХКФОМС для возобновления информационного взаимодействия;
- обратиться в ХКФОМС для расторжения Соглашения;
- обратиться в ХКФОМС за подтверждением подлинности Электронных подписей в Электронных документах.

ХКФОМС имеет право:

- запросить у Участника, а Участник обязан предоставить ХКФОМС сведения, необходимые для идентификации Пользователя (фамилия, имя, отчество (при наличии), должность, серия и номер документа удостоверяющего личность, СНИЛС, ИНН);
- отказать в регистрации Пользователя;
- отказать в удалении Пользователя в случае ненадлежащего оформления

заявления на удаление Пользователя;

- отказать в приостановлении информационного взаимодействия;
- отказать в возобновлении информационного взаимодействия;
- удалить Пользователя в случае установленного факта Компрометации ключевого набора, с уведомлением Участника и указанием причин;
- приостановить информационное взаимодействие с уведомлением Участника и указанием причин;
- запрашивать у Участника необходимую информацию, в том числе информацию о состоянии системы защиты информации Участника;
- проводить внеплановый контроль автоматизированных рабочих мест Участника, обрабатывающих сведения персонифицированного учета застрахованных лиц и (или) персонифицированного учета сведений о медицинской помощи, в целях проверки соблюдения требований по безопасности информации при обработке персональных данных и (или) их передачи по каналам связи с использованием средств криптографической защиты.

Участник обязан:

- самостоятельно произвести активацию дистрибутива ключей на своем рабочем месте;
- хранить в тайне личный пароль от дистрибутива ключей, принимать все возможные меры для предотвращения его раскрытия, искажения и несанкционированного использования;
- немедленно обратиться в ХКФОМС с заявлением на удаление Пользователя в случае раскрытия, искажения личного пароля от дистрибутива ключей, а также в случае, если Пользователю стало известно, что этот ключ используется или использовался ранее другими лицами;
- предоставлять ХКФОМС запрашиваемую информацию, в том числе информацию о состоянии системы защиты информации Участника;
- соблюдать требования Российского законодательства в области обеспечения безопасности информации.

ХКФОМС обязан:

- предоставить доступ к ресурсам ХКФОМС при соблюдении требований настоящего Регламента и законодательства в области обеспечения безопасности информации;
- организовать свою работу по GMT (Greenwich Mean Time, Среднее Время по Гринвичскому Меридиану) с учетом часового пояса и синхронизировать по времени все свои программные и технические средства обеспечения деятельности;
- уведомлять Участника о фактах, которые стали известны и которые существенным образом могут сказаться на возможности дальнейшего информационного взаимодействия;
- соблюдать требования Российского законодательства в области обеспечения безопасности информации.

4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доступ к ресурсам ХКФОМС при организации и ведении информационного взаимодействия в сфере обязательного медицинского страхования на территории Хабаровского края осуществляется по защищенным каналам связи с использованием программных и программно-аппаратных продуктов ViPNet.

Участники информационного взаимодействия обязаны выполнить требования по защите информации в соответствии с законодательством Российской Федерации о персональных данных.

Организационные и технические меры защиты информации, реализуемые в рамках информационного взаимодействия, должны быть направлены на исключение:

- неправомерного доступа к информации (обеспечение конфиденциальности информации);
- неправомерного уничтожения или модифицирования информации (обеспечение целостности информации);
- неправомерного блокирования информации (обеспечение доступности информации)
- возможности неконтролируемого проникновения или пребывания в помещениях лиц, не имеющих права доступа в эти помещения.

Для обеспечения защиты информации Участники проводят следующие мероприятия:

- формирование требований к защите информации;
- разработка системы защиты информации;
- внедрение системы защиты информации;
- обеспечение защиты информации в ходе эксплуатации информационной системы.

При этом организационные и технические меры защиты информации, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защиту среды виртуализации;
- защиту технических средств;

- защиту информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

На АРМ в обязательном порядке должно быть установлено лицензионное программное обеспечение.

Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации средства защиты информации. Средства защиты информации должны иметь действующие сертификаты соответствия ФСТЭК России и (или) ФСБ России.

Для внедрения единообразного механизма реализации информационного взаимодействия на АРМ должно использоваться программное обеспечение ViPNet Client, для работы в сети ViPNet № 620 или ведомственной защищенной сети передачи данных и средство электронной подписи КриптоПро CSP.

Должны приниматься необходимые правовые, организационные и технические меры или обеспечиваться их принятие для защиты информации ограниченного доступа, в том числе персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в соответствии с действующим законодательством Российской Федерации.

Участники самостоятельно обеспечивают установку и сопровождение СКЗИ у своих Пользователей.

Необходимо выполнять требования порядка ведения персонифицированного учета в сфере обязательного медицинского страхования, утвержденного приказом Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 N 29н "Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования" (зарегистрирован Министерством юстиции Российской Федерации 08.02.2011, регистрационный N 19742), в части наличия приказа, определяющего работников Участника, допущенных к работе с региональным сегментом единого регистра застрахованных лиц, соблюдение сроков передачи данных о застрахованных лицах и сведений об изменениях в этих данных в территориальный фонд, достоверность сведений, внесенных Участником в региональный сегмент единого регистра застрахованных лиц.

В соответствии с Федеральным законом от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании» и для выполнения требований приказа от 25.01.2011 г. № 29н «Об утверждении порядка ведения персонифицированного учета в сфере обязательного медицинского страхования», в части обеспечения безопасности персональных данных

застрахованных лиц, ХКФОМС оставляет за собой право внепланового проведения контроля автоматизированных рабочих мест Участника (Пользователя), обрабатывающих сведения персонифицированного учета застрахованных лиц и (или) персонифицированного учета сведений о медицинской помощи, в целях проверки соблюдения требований по безопасности информации при обработке персональных данных и (или) их передачи по каналам связи с использованием средств криптографической защиты.

Класс защищенности (уровень защищенности) подключаемой информационной системы должен быть не ниже класса защищенности (уровня защищенности) соответствующей информационной системы ХКФОМС. Информационной системе, обрабатывающей сведения персонифицированного учета застрахованных лиц, присвоен класс защищенности К3. Информационной системе, обрабатывающей персонифицированный учет сведений о медицинской помощи, присвоен класс защищенности К2.

5. ПОРЯДОК ПОДКЛЮЧЕНИЯ К ИНФОРМАЦИОННЫМ СИСТЕМАМ ХКФОМС

Техническое и информационное взаимодействие Участников предоставляется по решению директора ХКФОМС.

При подключении к информационным ресурсам ХКФОМС, Участник подключения обязан ознакомится с настоящим Регламентом и направить в ХКФОМС (посредством СЭД, почтового отправления, нарочно) Соглашение о присоединении к Регламенту (Приложение №1).

Организацию подключения информационных систем осуществляют Администраторы Участников.

5.1 Подключение пользователей сети ViPNet ХКФОМС

Для организации информационного обмена Участник информационного обмена направляет в ХКФОМС (посредством Деловой почты, СЭД, почтового отправления, нарочно) Запрос на регистрацию Пользователя (Приложение №2). Срок рассмотрения Запроса на регистрацию Пользователя и изготовления дистрибутива ключей – не более 5 рабочих дней.

Передача дистрибутива ключей может производиться лично Участнику информационного обмена или по каналам общего пользования «Интернет», с использованием средств криптографической защиты информации. Получателем дистрибутива ключей должен являться сотрудник Участника информационного обмена, имеющий право на получение. При получении дистрибутива ключей по «Деловой почте» необходимо приложенный к данному письму дистрибутив ключа скопировать на внешний носитель ("флэш") и хранить в недоступном месте (в сейфе или др.)

После получения дистрибутива ключей Участник – инициатор информационного обмена направляет в адрес ХКФОМС (посредством Деловой почты, СЭД, почтового отправления, нарочно) Уведомление о получении и установке дистрибутива ключей (Приложение №4). Уведомление подписывается лицом, ответственным за организацию работ по СКЗИ и утверждается руководителем Участника.

Установку дистрибутива ключей и настройку СКЗИ производит Администратор Участника самостоятельно.

Для добавления узлов защищенной сети ViPNet № 620 (адресатов Деловой почты, информационных ресурсов) необходимо сделать запрос в адрес Администратора сети ХКФОМС, с указанием Ф.И.О. адресата (для Деловой почты) или наименование узла (для информационных ресурсов).

5.2 Межсетевое взаимодействие

Межсетевое взаимодействие между ViPNet-сетью ХКФОМС и ViPNet-сетью Участника информационного взаимодействия, осуществляется через координаторы ViPNet-сетей Участников.

Межсетевое взаимодействие организуется с помощью межсетевого мастер-ключа, который формирует Администратор Участника инициатора информационного взаимодействия.

Межсетевое взаимодействие организуется в соответствии со структурной схемой защищенной сети Участника, подписанной уполномоченными представителями Участников. Структурная схема защищенной сети Участника выполняется в любом виде, с отображением узлов, участвующих в межсетевом взаимодействии и является приложением к Протоколу межсетевого взаимодействия (Приложение №5). Участники выбирают устройства (координаторы ViPNet-сетей), которые будут выполнять функции серверов-шлюзов при межсетевом взаимодействии, а также выделяют узлы своих ViPNet-сетей – абонентские пункты (автоматизированные рабочие места с установленным программным обеспечением ViPNet Client, далее – АП), – которые будут участвовать в межсетевом взаимодействии. Выделенные узлы сетей будут связаны в Центрах управления сетью взаимодействующих ViPNet-сетей. В случае если Участники включают в состав узлов, участвующих в межсетевом взаимодействии, автоматизированные рабочие места, на которых не установлено программное обеспечение ViPNet, при обмене информацией между Участниками применяется технология туннелирования.

В ЦУС ViPNet-сети № 620 (№ ____) в соответствии с «Руководство администратора ViPNet» производится формирование начального экспорта (ИСММК, справочная-ключевая информация), ViPNet-сети № 620 (№ ____) для ViPNet-сети № ____ (№ 620) (далее – начальный экспорт). Начальный экспорт доверенным способом передается в ЦУС ViPNet-сети № ____ (№ 620).

В ЦУС ViPNet-сети № ____ (№ 620) в соответствии с «Руководство администратора ViPNet» производится ввод и обработка (импорт) полученных из ЦУС ViPNet-сети № 620 (№ ____) данных (начального экспорта),

установление связей своих узлов с узлами ЦУС ViPNet-сети, предоставившего информацию. Далее в ЦУС ViPNet-сети № ____ (№ 620) создается ответная информация (ответный экспорт) для ЦУС ViPNet-сети № 620 (№ ____), приславшего первичную информацию.

Ответная информация (ответный экспорт) доверенным способом передается в ЦУС ViPNet-сети № 620 (№ ____), где она обрабатывается и вводится в действие. На этом этапе завершается процесс организации взаимодействия между ЦУС ViPNet-сети № 620 и ЦУС ViPNet-сети № ____, и дальнейший обмен данными между указанными ЦУС производится в автоматическом режиме посредством программного модуля ViPNet MFTP, входящего в состав ПК ViPNet.

После рассылки каждым ЦУС ViPNet-сетей Участников сформированных обновлений ключевой и справочной информации на свои узлы, участвующие в межсетевом взаимодействии, обеспечивается техническая возможность осуществления защищенного обмена между данными узлами информацией в электронной форме, и процедура установления межсетевого взаимодействия считается завершенной.

По окончанию процедуры межсетевого взаимодействия Участники составляют Протокол установления межсетевого взаимодействия (Приложение №5) с приложением структурных схем защищенной сети своей организаций. Протокол установления межсетевого взаимодействия составляется Участником – инициатором межсетевого взаимодействия. Протокол установления межсетевого взаимодействия составляется в двух экземплярах, по одной для каждой из Участников.

Модификация межсетевого взаимодействия осуществляется в соответствии с «Руководством администратора ViPNet» в следующих случаях:

- изменение состава узлов, участвующих в межсетевом взаимодействии;
- плановая смена межсетевого мастер-ключа;
- внеплановая смена межсетевого мастер-ключа;
- компрометация ключевой информации.

При подключения пользователя к сети ViPNet ХКФОМС посредством межсетевого взаимодействия и использованием СКЗИ сторонних производителей, Участник-инициатор подключения обязан направить (посредством Деловой почты, СЭД, почтового отправления, нарочно) Администратору сети ViPNet №620 копии Акта (актов) установки средств криптографической защиты информации.

6. ПРЕКРАЩЕНИЕ ТЕХНИЧЕСКОГО И (ИЛИ) ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

При выявлении нарушения требований настоящего Регламента, прекращается техническое взаимодействие между Участниками, с обязательным уведомлением о нарушении.

Для прекращения технического и (или) информационного взаимодействия Участник – инициатор уведомляет об этом Администратора сети ХКФОМС (посредством Деловой почты, СЭД, почтового отправления, нарочно) направляя ему Запрос на удаление Пользователя (Приложение №3). Администратор сети ХКФОМС незамедлительно производит удаление указанного Пользователя и узла.

Техническое и (или) информационное взаимодействие может быть расторгнуто по обоюдному согласию Участников, либо в одностороннем порядке с предупреждением другого Участника не позднее, чем за 30 календарных дней до расторжения Соглашения о присоединении к Регламенту.

7. СМЕНА КЛЮЧЕЙ В СЛУЧАЕ ИХ КОМПРОМЕТАЦИИ (ВНЕПЛАНОВАЯ СМЕНА КЛЮЧЕЙ)

К случаям компрометации относятся:

- утрата ключевых носителей;
- утрата ключевых носителей с их последующим обнаружением;
- прекращение полномочий или увольнение работников, имевших доступ к информационным системам ХКФОМС;
- возникновение подозрений об использовании АРМ, принадлежащего Пользователю без их согласия;
- нарушение оттиска печати на контейнерах или хранилищах с ключевыми носителями;
- нарушение пломб и печатей аппаратных средств АРМ;
- другие факты, свидетельствующие об утечке, модификации или блокировании ключевой информации.

При выявлении случаев компрометации ключевой информации, Пользователь самостоятельно принимает решение о компрометации своего набора ключей и принимает меры по недопущению угроз информационной безопасности при информационном взаимодействии. О возможном случае компрометации Пользователь немедленно сообщает своему Администратору. Администратор Участника, в случае установления факта компрометации, в течение 2 часов оповещает Администратора сети ХКФОМС по телефону, с обязательным уведомлением посредством электронной почты и прекращает использование скомпрометированного набора ключей. Посредством электронной почты Администратор Участника сообщает следующие сведения:

- полное наименование узла и Пользователя скомпрометированного ключа;
- причину прекращения информационного взаимодействия с данным Пользователем.

Администратор сети ХКФОМС в течение 24 часов производит удаление указанного Пользователя и узла.

При компрометации ключевого набора Участник обязан направить в ХКФОМС Приложение №3 - Запрос на удаление Пользователя. Запрос на удаление Пользователя направляется в ХКФОМС (посредством Деловой почты,

СЭД, почтового отправления, нарочно) не позднее трех рабочих дней с момента компрометации.

Возобновление информационного взаимодействия осуществляется в соответствии с п.5 настоящего Регламента.

8. ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ

Участники несут ответственность за использование полученной информации в соответствии с законодательством Российской Федерации.

При осуществлении технического и информационного взаимодействия ХКФОМС несет ответственность за доступность только тех узлов и информационных ресурсов, которые принадлежат сети ХКФОМС (сеть ViPNet №620).

Технически исправное состояние и работоспособность автоматизированных рабочих мест, участвующих в техническом и (или) информационном взаимодействии, Участники обеспечивают самостоятельно. Техническая поддержка программных продуктов, в том числе средств защиты информации, производится на основании Договоров (лицензий) на соответствующее ПО с соответствующим производителем.

В случае выявления нарушений требований по обеспечению безопасности персональных данных, нарушений порядка ведения персонифицированного учета в сфере обязательного медицинского страхования, а также нарушений при передаче конфиденциальной информации по каналам связи с использованием средств криптографической защиты информации принимается решение об ограничении доступа к информационным ресурсам ХКФОМС до устранения нарушений.

Участники не несут ответственность за неисполнение или ненадлежащее исполнение обязательств, принятых на себя в соответствии с настоящим Регламентом, если надлежащее исполнение оказалось невозможным вследствие наступления обстоятельств непреодолимой силы. Участники, в случае невозможности исполнения своих обязательств по причине наступления обстоятельств непреодолимой силы, должны предпринять все возможные действия для извещения другого Участника о наступлении таких обстоятельств. Исполнение обязательств возобновляется немедленно после прекращения действия обстоятельств непреодолимой силы.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ.

Возникновение Конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения Электронного документа, обнаружением возможной компрометации ключевого набора и иных случаях.

В случае возникновения обстоятельств, свидетельствующих, по мнению одного из Участника, о возникновении и/или наличии Конфликтной ситуации,

данный Участник (далее – Участник - инициатор) незамедлительно извещает другого заинтересованного Участника (далее – Участник – ответчик) о возможном возникновении и/или наличии Конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

Конфликтная ситуация признается разрешенной в случае, если Участник-инициатор удовлетворен информацией, полученной от Участника-ответчика, и не имеет к ней претензий в связи с Конфликтной ситуацией.

В случае если Участник-инициатор не удовлетворен информацией, полученной от Участника-ответчика, Участник-инициатор должен не позднее чем в течение двух рабочих дней после возникновения Конфликтной ситуации, направить Участнику-ответчику уведомление о Конфликтной ситуации (далее – Уведомление). Уведомление должно содержать:

- информацию о предмете и существе Конфликтной ситуации, обстоятельствах, по мнению Участника-инициатора, свидетельствующих о наличии Конфликтной ситуации, возможных причинах и последствиях ее возникновения;

- информацию, с указанием фамилий, имен, отчеств, должностей и контактной информации, должностных лиц Участника-инициатора, уполномоченных в разрешении Конфликтной ситуации (экспертная комиссия Участника – инициатора);

- информацию о предлагаемом месте, дате и времени сбора Участников, для Разрешения Конфликтной ситуации.

Участник – ответчик не позднее, чем на второй рабочий день после получения Уведомления направляет Участнику-инициатору Уведомление-ответ о Конфликтной ситуации. Уведомление должно содержать:

- информацию о предмете и существе Конфликтной ситуации, обстоятельствах, по мнению Участника-ответчика, свидетельствующих о наличии Конфликтной ситуации, возможных причинах и последствиях ее возникновения;

- информацию, с указанием фамилий, имен, отчеств, должностей и контактной информации, должностных лиц Участника-ответчика, уполномоченных в разрешении Конфликтной ситуации (экспертная комиссия Участника – ответчика);

- информацию о предлагаемом месте, дате и времени сбора Участников, для Разрешения Конфликтной ситуации;

Уведомления составляются на бумажном носителе, подписываются должностными лицами Участников (уполномоченными в разрешении Конфликтной ситуации) и передаются другому Участнику в установленном порядке, обеспечивающим подтверждение вручения корреспонденции. Уведомление может быть составлено и направлено в форме Электронного документа. При этом факт его доставки должен быть подтвержден.

Лица, входящие в состав Экспертной комиссии, должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения технического и информационного взаимодействия, построения и

функционирования Системы, организации и обеспечения информационной безопасности при техническом и информационном взаимодействии, должны иметь соответствующий допуск к необходимым для проведения работы Экспертной комиссии документальным материалам и программно-техническим средствам. В состав Экспертной комиссии назначаются представители служб информационно-технического обеспечения, служб обеспечения информационной безопасности, а также представители подразделений – исполнителей. По инициативе любого из Участника к работе Экспертной комиссии, для проведения технической экспертизы, могут привлекаться независимые эксперты, в том числе представители поставщиков средств защиты информации. При этом Участник, привлекающий независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг. При участии в Экспертной комиссии представителей сторонних органов и организаций, их право представлять соответствующие органы и организации должно подтверждаться официальным документом (доверенностью, предписанием, копией приказа или распоряжения).

Настоящим Регламентом устанавливается тридцатидневный срок работы Экспертной комиссии. В исключительных случаях срок работы Экспертной комиссии по согласованию Участников может быть дополнительно продлен не более чем на тридцать дней.

В ходе разрешения конфликтной ситуации Экспертная комиссия имеет право:

- получать доступ к необходимым для проведения ее работы документальным материалам Участников, на бумажных и электронных носителях;

- проводить ознакомление с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета Электронных документов;

- проводить ознакомление с условиями и порядком эксплуатации Участниками программно-технических средств, программного обеспечения и средств защиты информации;

-проводить ознакомление с условиями и порядком изготовления, использования и хранения Участниками ключевой информации, а также иной конфиденциальной информации и ее носителей, необходимых для работы Экспертной комиссии;

- получать объяснения от должностных лиц Участников информационного взаимодействия;

- получать от Участников любую иную информацию, относящуюся, по ее мнению, к рассматриваемой Конфликтной ситуации.

По итогам работы Экспертной комиссии составляется акт, при этом акт должен содержать следующую информацию:

- состав Экспертной комиссии;

- дату и место составления акта;

- даты и время начала и окончания работы Комиссией;

- описание конфликтной ситуации;

- фактические обстоятельства, установленные Комиссией;
- краткий перечень мероприятий, проведенных Комиссией;
- мероприятия Экспертной комиссии по проверке с применением аппаратно-программных средств (протоколы прилагаются к акту работы комиссии);
- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;
-подписи членов Экспертной комиссии.

К Акту может прилагаться особое мнение члена или членов Экспертных комиссий, не согласных с выводами Экспертной комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Экспертной комиссии, чье мнение оно отражает. Акт составляется в форме документа на бумажном носителе, по одному экземпляру каждому Участнику. По обращению любого из членов Экспертной комиссии, Участником, к которой было направлено обращение, ему должна быть выдана заверенная копия Акта.

Акт Экспертной комиссии является основанием для принятия Участниками решения по урегулированию Конфликтной ситуации.

10.ПРОВЕДЕНИЕ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ

Срок проведения профилактических мероприятий не должен превышать 2 суток.

Участники обязаны заблаговременно, не позднее чем за 3 дня до дня проведения профилактических мероприятий, оповестить о сроках проведения профилактических мероприятий.

11.ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

Изменения в настоящий Регламент вносятся по инициативе ХКФОМС.

При внесении изменений в настоящий Регламент и (или) схемы данных информационного взаимодействия, ХКФОМС обязан довести характер изменений, новую версию Регламента и (или) схемы данных информационного взаимодействия до Участников, участвующих в информационном взаимодействии, планируемую дату ввода в действие изменений. Уведомление осуществляется по электронной почте, а также путем размещения информационного сообщения на официальном сайте ХКФОМС. Соглашения, подписанные до внесения изменений, признаются действующими. В случае несогласия Участника с внесенными изменениями в Регламент, Участник вправе расторгнуть Соглашение. При расторжении Соглашения техническое и (или) информационное взаимодействие с данным Участником прекращается.

12.ИНЫЕ ОБСТОЯТЕЛЬСТВА

Иные обстоятельства, не отраженные в данном Регламенте, рассматриваются в индивидуальном порядке.

13. КОНТАКТЫ

Заведующий сектором по защите информации	8 (4212) 97-03-63
Администратор сети ViPNet №620	8 (4212) 97-03-65
Деловая почта сеть ViPNet №620	027(ХКФОМС) Администратор Центра Управления Сетью
Приемная ХКФОМС	8 (4212) 97-03-00
ХКФОМС	680000, г. Хабаровск, ул. Фрунзе, д. 69

Приложение №1

Соглашение о присоединении к Регламенту технического и информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования

«__»_____ 20___ г. г. Хабаровск

Краевое государственное бюджетное учреждение здравоохранения «Городская поликлиника» управления здравоохранения администрации г. Хабаровска в лице главного врача Иванова Ивана Ивановича действующего на основании Устава *(распоряжения, постановления, приказа или др.)* с одной стороны, и Хабаровский краевой фонд обязательного медицинского страхования, в лице директора Пузаковой Елены Викторовны, действующего на основании распоряжения Губернатора Хабаровского края от 14.09.2012 г. №142-рк, с другой стороны, совместно именуемые Стороны, заключили настоящее Соглашение о техническом и информационном взаимодействии в соответствии с Регламентом технического и информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования (далее – Регламент).

Настоящим Соглашением Стороны признают Регламент и обязуются выполнять его требования.

Соглашение составлено в 2-х (двух) экземплярах, имеющих одинаковую юридическую силу – по одному для каждой из Сторон.

Настоящее Соглашение вступает в силу с даты его подписания Сторонами действует до его расторжения по основаниям, предусмотренным законодательством Российской Федерации, или по решению любой из Сторон, подписавших Соглашение, в одностороннем внесудебном порядке.

АДРЕСА И РЕКВИЗИТЫ СТОРОН

Краевое государственное бюджетное учреждение здравоохранения «Городская поликлиника»	Хабаровский краевой фонд обязательного медицинского страхования
680000 г. Хабаровск,	680000, г. Хабаровск,
ул. Ленина, д.00	ул. Фрунзе, д.69
Телефон: (4212) 00-00-00	Телефон: (4212) 97-03-00
Тел./Факс: (4212) 00-00-00	Тел./Факс: (4212) 32-92-45
Главный врач КГБУЗ «ГП»	Директор ХК ФОМС
_____/И.И. Иванов	_____ / Е.В. Пузакова
м.п.	м.п.

Приложение №2

Заместителю директора ХКФОМС по защите информации и правовому обеспечению

И.А. Буднику

680000, г. Хабаровск, ул. Фрунзе, д.69

Запрос на регистрацию пользователя

Краевое государственное бюджетное учреждение здравоохранения «Городская поликлиника» управления здравоохранения администрации г. Хабаровска в лице главного врача Иванова Ивана Ивановича действующего на основании Устава *(распоряжения, постановления, приказа или другое)*, просит зарегистрировать своего сотрудника Пользователем сети ViPNet №620 ХКФОМС в соответствии с указанными в настоящем запросе данными:

Фамилия Имя Отчество	Сидоренко Сергей Сидорович
ИНН*	270011223344
СНИЛС*	123-456-789-01
Должность	медицинский регистратор
Подразделение	регистратура
Полное наименование организации	КГБУЗ «Городская поликлиника» министерства здравоохранения Хабаровского края
Почтовый адрес организации (подразделения)	680000, г. Хабаровск, ул. Неизвестная, д. 100
Адрес электронной почты	kgbuz@mail.ru
Область:	Хабаровский край
Контактный телефон системного администратора	8-914-000-00-00

* Заполняется при необходимости назначить данному сотруднику роль «Деловая почта»

С Регламентом информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа. Соглашаюсь с обработкой своих персональных данных для обеспечения информационного взаимодействия и что мои персональные данные, предоставляемые в Хабаровский краевой фонд обязательного медицинского страхования, будут относиться к общедоступным персональным данным, участников информационного взаимодействия.

Пользователь УЦ ХКФОМС: _____ / С.С. Сидоренко / « ___ » _____ 202__ г.	Заверяю подпись Пользователя УЦ ХКФОМС Главный врач _____ / И.И. Иванов / « ___ » _____ 202__ г. *М.П.*

Настоящим подтверждаю, что Запрос на регистрацию пользователя получен.

Уполномоченное лицо ХКФОМС:

_____ / _____ /

«____» _____ 202__г.

Приложение №3

Заместителю директора ХКФОМС по защите информации и правовому обеспечению

И.А. Буднику

680000, г. Хабаровск, ул. Фрунзе, д.69

Запрос на удаление пользователя

В соответствии с Регламентом информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования, Краевое государственное бюджетное учреждение здравоохранения «Городская поликлиника» управления здравоохранения администрации г. Хабаровска в лице главного врача Иванова Ивана Ивановича действующего на основании Устава *(распоряжения, постановления, приказа или другое)*, в связи с ***(выбрать:** переводом на другую должность, компрометацией пользователя, увольнением или другое)*, просит удалить следующего пользователя сети VipNet №620:

Полное наименование абонентского пункта	027 (270000) КГБУЗ «ГП» АП1
Фамилия Имя Отчество	Сидоров Сергей Сидорович
Адрес электронной почты Организации	kgbuz@mail.ru

Также сообщаем, что 26.12.2019 г. комиссия в составе: Главный врач КГБУЗ «ГП» Иванов И.И. и главный специалист Анисимов А.А. произвела уничтожение ключевой информации, дистрибутив ключей № abn_094e.dst, содержащий информацию об узле «027(270000) КГБУЗ ГП АП3» пользователя «Кистина Ю.С.», о чем сделана запись в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Главный врач КГБУЗ «ГП» _____ / И.И. Иванов /

«___»_____202__г.

М.П.

Приложение №4

Заместителю директора ХКФОМС по защите информации и правовому обеспечению

И.А. Буднику

680000, г. Хабаровск, ул. Фрунзе, д.69

Уведомление о получении и установки дистрибутива ключей

В соответствии с Регламентом информационного взаимодействия Хабаровского краевого фонда обязательного медицинского страхования направляем настоящее уведомление.

Дата получения дистрибутива	Наименование файл-ключа (*.dst)	Ф.И.О. пользователя	Наименование АП	Место установки (адрес)
01.01.2020	abn_094e.dst	Сидоров Е.А.	027 (270000) КГБУЗ «ГП» АП1	г. Хабаровск, ул. Сидорова, д.1

Ответственный за организацию работ по СКЗИ _____/Петров А.А./

Главный врач КГБУЗ «ГП» _____ / И.И. Иванов /

« __ » _____ 202__ г.

М.П.

Приложение №5

ПРОТОКОЛ
установления межсетевого взаимодействия

г. Хабаровск «___»_____20___г.

1. Целью установления межсетевого взаимодействия является защищенное информационное взаимодействие ViPNet-сетей указанных организаций.

2. Межсетевое взаимодействие установлено между сетями:

Номер сети ViPNet	Полное наименование организации
№ 620	Хабаровский краевой фонд обязательного медицинского страхования
№____	Наименование организации

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети ViPNet	Должность	Ф.И.О.	Контактный телефон
№ 620			
№ ___			

4. Передача начального и ответного экспорта между сетями № 620 и №____ осуществлялась через специалиста, уполномоченного Сторонами на данные действия.
5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети № 620.
6. При установлении межсетевого взаимодействия были произведены импорты справочно-ключевой информации абонентов сети № 620 и сети № ____.

Приложение: 1. Структурная схема защищенной сети ХКФОМС
2. Структурная схема защищенной сети наименование организации

Начальник отдела программно-технического обеспечения ХКФОМС

_____/_____/

Руководитель подразделения

_____/_____/

Ответственный специалист

_____/_____/

Ответственный специалист

_____/_____/

Приложение 1.

Структурная схема защищенной сети ХКФОМС

Приложение 2.

Структурная схема защищенной сети наименование организации