РЕГЛАМЕНТ
ЗАЩИЩЁННОЙ ВИРТУАЛЬНОЙ СЕТИ VIPNET ТЕРРИТОРИАЛЬНОГО ФОНДА ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ МУРМАНСКОЙ ОБЛАСТИ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ViPNet [Администратор]	-	программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой сетью ViPNet.
ViPNet [Клиент]	-	программное обеспечение, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента, персонального экрана и клиента защищённой почтовой службы.
ViPNet [Координатор]	-	программное обеспечение, выполняющее функции универсального сервера виртуальной защищённой сети ViPNet.
VPN (Virtual Private Network)	-	обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.
Абонент Защищённой сети	-	назначенный приказом руководителя, сотрудник Участника системы здравоохранения, использующий для выполнения своих служебных обязанностей сервисы и информационные системы Защищённой сети.
Абонентский пункт	-	персональный компьютер с установленным программным обеспечением ViPNet [Клиент].
Автопроцессинг	-	автоматическая обработка файлов и писем в программе «Деловая почта», в соответствии с различными правилами, задаваемыми пользователем.
Владелец информационных систем	-	участник, осуществляющий владение и пользование информационными системами и реализующий полномочия распоряжения в пределах, установленных законодательством.
Владелец сертификата ключа проверки электронной подписи	-	физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).
Главный администратор Защищённой сети	-	Назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области осуществляющий общую политику администрирования всей Защищённой сети.
Информационная система	-	совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Ключ проверки электронной подписи	-	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).
Ключ электронной подписи	-	уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.
Ключевой носитель	-	носитель, содержащий один или несколько ключей.
Компрометация ключа	-	утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.
Координатор Защищённой сети	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области, определяющий общую стратегию развития Защищённой сети.
Корпоративная информационная система ТФОМС Мурманской области	-	Информационная система, участниками электронного взаимодействия в которой являются Участники системы здравоохранения.
Локальный администратор Защищённой сети	-	назначенный приказом сотрудник Участника системы здравоохранения, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному участнику.
Несанкционированный доступ	-	доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах путём изменения (повышения, фальсификации) своих прав доступа.
Пользователь Удостоверяющего центра	-	физическое лицо (уполномоченный представитель Участника присоединившегося к Регламенту Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области), зарегистрированное в Удостоверяющем центре.

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.
Список отозванных сертификатов	-	документ на бумажном носителе или электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения их срока действия.
Средство электронной подписи	-	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. В Защищённой сети, данные функции реализованы в модуле «Деловая почта».
Технология ViPNet	-	технология, предназначенная для построения виртуальных защищённых сетей, путём использования системы персональных и межсетевых экранов на защищаемых компонентах распределённой сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе средства криптографической защиты информации «Домен-К».
Удостоверяющий центр	-	Территориальный фонд обязательного медицинского страхования Мурманской области, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством.
Уполномоченное лицо Удостоверяющего центра	-	назначенный приказом директора сотрудник Территориального фонд обязательного медицинского страхования Мурманской области, наделённый полномочиями по заверению сертификатов ключей проверки электронных подписей и списков отозванных сертификатов.
Усиленная неквалифицированная электронная подпись (далее – неквалифицированная ЭП)	-	ЭП, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания.

Участник системы здравоохранения	-	обладатель информации, формирующейся в области здравоохранения, осуществляющий деятельность, направленную на реализацию прав граждан на охрану здоровья и медицинскую помощь.
Центр управления сетью	-	аппаратные или программные средства для мониторинга, конфигурирования и управления узлами защищённой сети.
Электронная подпись (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.
Электронный документ	-	документ, в котором информация представлена в электронно-цифровой форме, и который может быть представлен в виде файла, хранящегося на носителе.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Регламент защищённой виртуальной сети VipPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Регламент) разработан в соответствии с:

- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской федерации»;
- Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Регламент определяет и устанавливает:

-порядок организации и подключения Участников Защищенной сети (далее – Участники) к защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Защищённая сеть);

-порядок предоставления доступа к информационным системам Защищённой сети;

-порядок организации защищённого межсетевого взаимодействия;

-порядок разрешения конфликтных ситуаций.

3. ПОРЯДОК ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ УЧАСТНИКОВ К ЗАЩИЩЁННОЙ СЕТИ

3.1 Организация подключения Участников к Защищённой сети включает в себя следующие стадии:

-заявительная стадия;

-стадия рассмотрения заявления;

-закупка программного обеспечения;

-формирование и передача ключевой информации;

-формирование и передача учётных записей для доступа к информационным системам.

3.2 Заявительная стадия.

Участник, желающий подключиться к Защищённой сети (далее – Претендент) направляет в адрес ТФОМС Мурманской области заявление о намерении подключиться к Защищённой сети (Приложение №1).

3.2.1 В заявлении должна содержаться следующая информация:

-предполагаемое количество подключаемых Абонентских пунктов;

-общий перечень Участников, с которыми необходима организация защищённого обмена;

-перечень информационных систем, к которым необходимо организовать доступ;

-ФИО и контактный телефон лица, ответственного за подключение Претендента.

3.3 Стадия рассмотрения заявления

3.3.1 ТФОМС Мурманской области в течение 3-х рабочих дней со дня получения заявления о намерении подключиться к Защищённой сети, проводит оценку оснований для подключения Претендента к Защищённой сети, технической возможности организации направлений связи и доступа к информационным системам.

3.3.2 Приобретение программного обеспечения ViPNet [Клиент], до рассмотрения заявления о намерении подключиться к Защищённой сети, не является основанием и гарантией подключения Претендента к Защищённой сети.

3.3.3 Решение о подключении Претендента к Защищённой сети, направляется в письменной форме в адрес Претендента в течение 3-х рабочих дней со дня принятия указанного решения.

3.3.4 ТФОМС Мурманской области имеет право отказать Претенденту в подключении к Защищённой сети, объяснив причину отказа. Решение об отказе в подключении Претендента к Защищённой сети направляется в письменной форме в адрес Претендента в течение 3-х рабочих дней со дня принятия указанного решения.

3.3.5 ТФОМС Мурманской области уведомляет Претендента о принятии решения о подключении (отказе в подключении) к Защищённой сети, посредством электронной почты, указанной в заявление о намерении подключиться к Защищённой сети, со ссылкой на соответствующее решение.

3.4. Закупка программного обеспечения ViPNet [Клиент] Претендентом.

3.4.1 В случае принятия положительного решения о подключении к Защищённой сети, Претендент самостоятельно приобретает программное обеспечение ViPNet [Клиент].

3.4.2 При оформлении договорных отношений по приобретению программного обеспечения ViPNet [Клиент] Претендент указывает номер Защищённой сети для подключения - 613.

3.4.3 Подключение Претендента к Защищённой сети осуществляется ТФОМС Мурманской области, только после получения регистрационных файлов от производителя программного обеспечения или представителя производителя программного обеспечения.

3.4.4 ТФОМС Мурманской области уведомляет Претендента о получении регистрационных файлов.

3.5 Формирование и передача ключевой информации.

3.5.1 Претендент после получения информации о поступлении регистрационных файлов, формирует и направляет в ТФОМС Мурманской области заявку на подключение (Приложение №2)

3.5.2 В течение 3 рабочих дней со дня получения от Претендента заявки на подключение ТФОМС Мурманской области:

-производит регистрацию Абонентских пунктов и Абонентов в Центре управления сетью;

-организовывает направления связи между Абонентскими пунктами, в соответствии с заявкой на подключение;

-формирует дистрибутивы ключей для Абонентских пунктов вместе с паролем доступа к нему;

-по завершению обозначенных работ уведомляет об этом Претендента.

3.5.3 Претендент для получения дистрибутива ключей и пароля доступа к нему должен:

а) Предоставить в адрес ТФОМС Мурманской области:

-копию приказа о назначении Локального администратора (Приложение №3) и Абонентов Защищённой сети (Приложение №4);

-копии соглашений с Локальным администратором и Абонентами Защищённой сети о неразглашении информации, к которой будет получен доступ в связи с выполнением своих функций (Приложение №5);

б) Направить в ТФОМС Мурманской области Локального администратора с доверенностью на получение дистрибутива ключей (Приложение №6).

3.5.5. Факт выдачи дистрибутива ключей, заносится в Журнал учёта выдачи ключевых документов (Приложение №7).

3.5.4 Претендент для получения доступа к информационным системам Участников, должен предоставить в адрес ТФОМС Мурманской области копию документа, подтверждающего согласие Владельца информационной системы (далее - Владельца) на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является ТФОМС Мурманской области - не требуется).

3.6 Формирование и передача учётных записей для доступа к информационным системам.

Локальный администратор Владельца информационной системы формирует учётные записи для доступа и передаёт их Локальному администратору Претендента в сроки и на согласованных ими условиях.

4. ПОРЯДОК ИЗМЕНЕНИЯ НАПРАВЛЕНИЙ СВЯЗИ И/ИЛИ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

4.1 Порядок изменения направлений связи и/или предоставление доступа к информационным системам включает в себя следующие стадии:

-заявительная стадия;

-стадия рассмотрения заявления;

-формирование и передача ключевой информации;

-формирование и передача учётных записей для доступа к информационным системам.

4.2 Заявительная стадия.

4.2.1 Участник желающий изменить направление связей и/или получить доступ к информационным системам Защищённой сети направляет в адрес ТФОМС Мурманской области заявку за подписью руководителя (Приложение №8) и копию документа подтверждающего согласие Владельца на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является ТФОМС Мурманской области - не требуется).

4.2.2 При заполнении заявки следует указывать все необходимые на данный момент направления связи и все информационные системы Защищённой сети, к которым необходим доступ.

4.3 Рассмотрение заявки.

4.3.1 ТФОМС Мурманской области в течение 3-х рабочих дней со дня получения рассматривает заявку, проводит оценку технической возможности для изменения направлений связи и/или организации доступа к информационным системам Защищённой сети.

4.3.2 Решение об изменении направлений связи и/или организации доступа к информационным системам Защищённой сети, направляется в письменной форме в адрес Участника в течение 3-х рабочих дней со дня принятия указанного решения.

4.3.3 ТФОМС Мурманской области имеет право отказать Участнику в изменении направлений связи и/или организации доступа к информационным системам Защищённой сети, объяснив причину отказа. Решение об отказе в изменении направлений связи и/или организации доступа к информационным системам Защищённой сети направляется в письменной форме в адрес Участника в течение 3-х рабочих дней со дня принятия указанного решения.

4.3.4. ТФОМС Мурманской области уведомляет Претендента об изменении направлений связи и/или организации доступа к информационным системам Защищённой сети, посредством электронной почты, со ссылкой на соответствующее Решение.

4.4 Формирование и передача ключевой информации

4.4.1 В течение 5 рабочих дней со дня уведомления Участника о принятии решения об изменении направлений связи и/или организации доступа к информационным системам Защищённой сети ТФОМС Мурманской области:

-вносит изменения в направления связей между Абонентскими пунктами, в соответствии с заявлением;

-формирует необходимую справочную и ключевую информацию;

-через Центр управления сетью направляет справочную и ключевую информацию на соответствующие Абонентские пункты Участника;

-по завершению обозначенных работ уведомляет об этом Участника.

4.4.2 При поступление на Абонентский пункт новая ключевая информация автоматически обновляет существующую ключевую информацию.

4.5 Формирование и передача учётных записей для доступа к информационным системам.

Локальный администратор Владельца формирует учётные записи для доступа к информационным системам и передаёт их Локальному администратору Участника в сроки и на согласованных ранее условиях.

5. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ СЕТЯМИ VIPNET

5.1 Организация межсетевого взаимодействия с другими сетями ViPNet включает в себя следующие стадии:

-заявительная стадия;

-рассмотрение заявления;

-формирование и передача ключевой информации;

5.2 Заявительная стадия.

5.2.1 Для организации межсетевого взаимодействия между Защищённой сетью и сторонней сетью ViPNet, Координатор Защищённой сети или администратор сторонней ViPNet сети готовят информационное письмо, в котором информируют другую сторону о необходимости организации информационного межсетевого взаимодействия с указанием контактов лиц ответственных за организацию межсетевого взаимодействия.

5.3 Рассмотрение заявления.

5.3.1 ТФОМС Мурманской области в течение 3-х рабочих дней со дня получения информационного письма проводит оценку оснований и технической возможности для организации межсетевого взаимодействия.

5.3.2 ТФОМС Мурманской области имеет право отказать в организации межсетевого взаимодействия, объяснив причину отказа.

5.3.3 В случае принятия решения об организации межсетевого взаимодействия ТФОМС Мурманской области в течении 5-ти рабочих дней в письменной форме уведомляет о принятии такого решения организацию инициирующую данное взаимодействие.

5.4 Формирование и передача ключевой информации.

5.4.1 В случае принятия решения об организации межсетевого взаимодействия, Главный администратор и администратор сторонней сети ViPNet, в соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]» производят формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая корневые сертификаты для каждой их сетей.

5.4.2 Указанные данные (начальный экспорт) доверенным способом передаются в соответствующие Центры управления сетей (далее – ЦУС), с которыми должно осуществляться межсетевое взаимодействие.

5.4.3 Во всех ЦУС в соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]» производится ввод и обработка (импорт) полученных из других ЦУС данных (начального экспорта), установление связей своих Абонентских пунктов с Абонентскими пунктами ЦУС, предоставившими информацию (ответный экспорт) для ЦУС, приславших первичную информацию, включая свои сертификаты.

5.4.4 Ответная информация (ответный экспорт) доверенным способом передаются в соответствующие ЦУС, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межсетевого взаимодействия между ЦУС, в дальнейшем обмен данными между ними производится в автоматическом режиме.

5.4.5 Сформированная ключевая и справочная информация через ЦУС отправляется на Абонентские пункты, участвующие в межсетевом взаимодействии.

5.4.6 После завершения процедуры организации межсетевого взаимодействия между Защищённой сетью и сторонней сетью ViPNet, подписывается Протокол установления межсетевого взаимодействия (Приложение №9).

5.5 Организация направлений связи между Абонентскими пунктами Участников и Абонентскими пунктами сторонней сети ViPNet, с которой установлено межсетевое взаимодействие, осуществляется в соответствии с разделом 4 настоящего Регламента.

5.6 При каждой модификации межсетевого взаимодействия Главный администратор заносит соответствующие записи в Журнал изменений межсетевого взаимодействия (Приложение №10).

6. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ ПЛАНОВОЙ СМЕНЫ МЕЖСЕТЕВОГО МАСТЕР-КЛЮЧА.

6.1 Порядок модификации межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа предполагает выполнение ряда технологических и организационных мероприятий.

6.2 Предварительные организационные мероприятия.

Перед тем как осуществлять плановую смену межсетевого мастер-ключа, Главный администратор и администратор сторонней сети ViPNet, с которой установлено межсетевое взаимодействие должны:

-выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями;

-в случае использования симметричного мастер-ключа выбирается сеть, в которой будет создан новый межсетевой мастер-ключ;

-выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для Абонентских пунктов сетей.

6.3 Формирование нового межсетевого мастер-ключа.

Формирование нового межсетевого мастер-ключа производится в соответствии с «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]»

6.4 Процедура создания экспорта и приёма импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных и приём импортированных данных в соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]».

6.5 Межсетевое взаимодействие после смены межсетевого мастер-ключа.

После смены межсетевого мастер-ключа связь между взаимодействующими Абонентскими пунктами Защищённой сети и ViPNet сети, с которой установлено межсетевое взаимодействие, возможна только после прохождения обновления ключевой информации на всех соответствующих Абонентских пунктах.

6.6 Обновленная ключевая информация через ЦУС отправляется на Абонентские пункты, участвующие в межсетевом взаимодействии.

6.7 Записи в журнале изменений межсетевого взаимодействия.

После смены межсетевого мастер-ключа Главный администратор заносит соответствующие записи в Журнал изменений межсетевого взаимодействия.

7. НАЗНАЧЕНИЕ ОТВЕТСТВЕННЫХ ЛИЦ

7.1 Назначение Координатора.

7.1.1 Исполнение функций Координатора возлагается на сотрудника ТФОМС Мурманской области.

7.1.2 Координатор назначается и отстраняется от исполнения возложенных функций, приказом директора ТФОМС Мурманской области.

7.1.3 Функции и полномочия Координатора определены в разделе 7 Положения о Защищённой виртуальной сети Территориального фонда обязательного медицинского страхования Мурманской области (далее – Положения).

7.2 Назначение Главного администратора.

7.2.1 Исполнение функций Главного администратора возлагается на сотрудника ТФОМС Мурманской области.

7.2.2 Главный администратор назначается и отстраняется от исполнения возложенных функций, приказом директора ТФОМС Мурманской области.

7.2.3 Функции и полномочия Главного администратора определены в разделе 8 Положения.

7.3 Назначение Локального администратора.

7.3.1 Исполнение функций Локального администратора возлагается на сотрудника Участника.

7.3.2 Локальный администратор назначается и отстраняется от исполнения возложенных функций приказом руководителя Участника.

7.3.3 Функции и полномочия Локального администратора определены в разделе 9 Положения.

7.3.4 Необходимым условием назначения Локального администратора, является подписание с ним соглашения о неразглашении информации, полученной вследствие выполнения своих обязанностей.

7.3.5 В случае смены сотрудника на, которого возложены функции Локального администратора, Участник обязан в течение 2-х рабочих дней известить об этом Координатора, направив заявку (Приложение №11) и Владельца информационных систем, к которым Участник имеет доступ.

7.3.6 При заполнении заявки, необходимо указывать всех назначенных на данный момент Локальных администраторов и Абонентов Участника.

7.3.7 Главный администратор в течение 1-го рабочего дня создаёт новые ключевые наборы для всех Абонентов Участника и передаёт их Локальному администратору.

7.3.8 Локальный администратор Владельца информационных систем, к которым Участник имеет доступ, блокирует старые и создаёт новые учётные записи всех Абонентов Участника для доступа к информационным системам в сроки и на согласованных ими условиях.

7.3.9 Копию приказа о возложении функций Локального администратора на сотрудника Участника, а также копию подписанного с этим сотрудником, соглашения о неразглашении информации полученной вследствие выполнения своих обязанностей, передаются Участником Координатору.

7.4 Назначение Абонентов.

7.4.1 Список сотрудников (Абонентов), которым для выполнения служебных обязанностей необходим доступ в Защищённую сеть, утверждается приказом руководителя Участника.

7.4.2 С каждым сотрудником (Абонентом) допущенным к работе в Защищённой сети, подписывается соглашение о неразглашении информации полученной вследствие выполнения своих должностных обязанностей.

7.4.3 В случае изменения списка сотрудников (Абонентов), которым для выполнения служебных обязанностей необходим доступ в Защищённую сеть, Участник обязан известить об этом Координатора, направив заявку (Приложение №11) и Владельца информационных систем, к которым Участник имеет доступ в течение 2-х рабочих дней.

7.4.4 При заполнении заявки, необходимо указывать всех назначенных на данный момент Локальных администраторов и Абонентов Участника.

7.4.5 Главный администратор в течение 1-го рабочего дня создаёт новые ключевые наборы вновь назначенных Абонентов Участника и передаёт их Локальному администратору.

7.4.6 Локальный администратор Владельца информационных систем, к которым Участник имеет доступ, блокирует старые и создаёт новые учётные записи для вновь назначенных Абонентов Участника для доступа к информационным системам в сроки и на условиях оговорённых заранее.

7.4.7 Копии приказов об утверждении списка сотрудников, которым для выполнения служебных обязанностей необходим доступ в Защищённую сеть, а также соглашения о неразглашении информации полученной вследствие выполнения своих должностных обязанностей, подписанных с этими сотрудниками, передаются Участником Координатору.

8. КОМПРОМЕТАЦИЯ КЛЮЧЕЙ

8.1 К событиям компрометации, когда ключи Абонента считаются скомпрометированными, относятся следующие случаи:

- посторонним лицам мог стать доступен (стал доступен) файл ключевого дистрибутива Абонента;
- посторонним лицам мог стать доступен (стал доступен) съёмный носитель ключевой информации Абонента;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Абонентском пункте;
- на Абонентском пункте отсутствовал (был отключен) модуль ViPNet Client Monitor, или он устанавливался в 4-й или 5-й режим, и в локальной сети считается возможным присутствие посторонних лиц;
- прекращение полномочий Абонента или Локального администратора, согласно соответствующего приказа, имевшего доступ к паролям и ключам, в том числе в связи с расторжением трудового договора (договора возмездного оказания услуг).

8.2 При возникновении сомнений в неизвестности посторонним лицам пароля доступа Абонента при старте модуля ViPNet Client Monitor, при условии, что доступ к Абонентскому

пункту посторонних лиц был невозможен, Локальному администратору следует сменить пароль и разрешить Абонентам продолжить работу.

8.3 При возникновении сомнений в неизвестности посторонним лицам пароля доступа Абонента при старте модуля ViPNet Client Monitor, при условии, что доступ к Абонентскому пункту посторонних лиц был возможен, ключи считаются скомпрометированными.

8.4 К событиям, требующим проведения расследования и принятия решения на предмет компрометации ключевой информации, относится возникновение подозрений в утечке информации при её передаче посредством защищённой сети.

8.5 В случае прекращения полномочий Абонента, ключи данного Абонента считаются скомпрометированными.

8.6 В случае прекращения полномочий Локального администратора, ключевая информация всех Абонентов Участника считается скомпрометированной.

8.7 В случае наступления любого из событий, связанных с компрометацией ключевой информации, Абонент немедленно прекращает связь с другими Абонентскими пунктами и сообщает о факте компрометации своему Локальному администратору.

8.8 Локальный администратор доводит информацию о факте компрометации (или предполагаемом факте компрометации) до Главного администратора.

8.9 Главный администратор при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

-в программном обеспечение ViPNet [Администратор] объявить ключи Абонентского пункта скомпрометированными и создать средствами программного обеспечения справочники связей при компрометации с необходимой информацией;

-оповестить о факте компрометации ключей всех Абонентов, связанных с Абонентом ключевая информация которого была скомпрометирована;

-сформировать средствами программного обеспечения ViPNet [Администратор] новую ключевую информацию. Все файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи;

-произвести рассылку сформированных обновлений ключей на Абонентские пункты Защищённой сети.

9. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

9.1 Компрометация ключей Абонента.

При наступлении любого из перечисленных в п. 8.1 настоящего Регламента событий Абонент, должен немедленно прекратить работу на своём Абонентском пункте и сообщить о факте компрометации администратору своей сети ViPNet.

9.1.1 Администратор сети ViPNet при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

-в программном обеспечение ViPNet [Администратор] объявить ключи Абонентского пункта скомпрометированными и создать средствами программного обеспечения справочники связей при компрометации с необходимой информацией;

-оповестить о факте компрометации ключей всех Абонентов, связанных с Абонентом ключевая информация которого была скомпрометирована;

-сформировать средствами программного обеспечения ViPNet [Администратор] новую ключевую информацию. Все файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи;

-произвести рассылку сформированных обновлений ключей на Абонентские пункты Защищённой сети.

-сформировать и отправить импорт для сети ViPNet, с Абонентскими пунктами которой, взаимодействовал скомпрометированный Абонентский пункт;

9.1.2 Администратор ViPNet сети, Абоненты которой взаимодействовали с Абонентом, ключи которого скомпрометированы, после приёма и обработки импорта создаёт новую ключевую информацию своим Абонентам.

9.1.3 Возобновление межсетевого взаимодействия возможно только после прохождения обновления ключевой информации на всех взаимодействующих Абонентских пунктах.

9.2 Внеплановая смена межсетевого мастер-ключа.

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации межсетевого мастер ключа, на котором происходит организация межсетевого взаимодействия.

9.2.1 В случае компрометации симметричного межсетевого мастер-ключа считается скомпрометированной вся ключевая информация, которая используется при защищённом межсетевом взаимодействии. межсетевое взаимодействие должно быть немедленно остановлено.

9.2.2 Для восстановления работы межсетевого взаимодействия необходимо произвести технологические и организационные мероприятия, описанные в разделе 6 «Порядок организации защищённого межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа».

9.2.3 При компрометации ключей Главный администратор заносит соответствующие записи в Журнал изменений межсетевого взаимодействия.

10. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

10.1 Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения Участниками электронных документов и/или получение доступа к информационным системам других Участников.

10.2 Разрешение конфликтных ситуаций осуществляется путём взаимодействия Локальных администраторов Участников, у которых возникли претензии.

10.3 В случае необходимости, для разрешения конфликтных ситуаций, могут быть привлечены Координатор и Главный администратор.

ОБРАЗЕЦ

Приложение №1
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

Директору
Территориального фонда обязательного
медицинского страхования Мурманской
области

Акульчеву В.А.

О подключении
к защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

Прошу подключить _*Муниципальное учреждение здравоохранения «Городская поликлиника №1234» г. Мурманск* к защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области для обмена информацией, содержащей персональные данные, со *страховыми медицинскими организациями г. Мурманска, Мурманским областным медицинским информационно-аналитическим центром, Территориальным фондом обязательного медицинского страхования Мурманской области, Комитетом по здравоохранению г. Мурманск.*

Предполагаемое число подключаемых абонентских пунктов – *2 (два).*

Перечень информационных систем, к которым необходим доступ: *Единый регистр застрахованного населения Мурманской области.*

Лицо, ответственное за подключение, и контактный телефон: *Иванов Иван Иванович*, *(8 815) 22-22-22, адрес электронной почты*

Руководитель организации _____ /ФИО/

М.П.

ОБРАЗЕЦ

Приложение №2
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на подключение к Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского страхования
Мурманской области.

	Директору Территориального фонда обязательного медицинского страхования Мурманской области Акульчеву В.А.
1. Полное наименование организации без сокращений (на основании учредительных документов)	
Муниципальное учреждение здравоохранения «Городская поликлиника №1234» г. Мурманск	
2. Сокращённое название организации	
МУЗ «Городская поликлиника №1234»	
3. Юридический адрес организации с индексом	
г. Мурманск, ул. Северная 1, 184111	
4. Фактический (почтовый) адрес организации с индексом	
г. Мурманск, ул. Северная 1, 184111	
5. ФИО руководителя	
Петров Пётр Петрович	
6. Должность руководителя	
Главный врач	
7. Количество необходимых для регистрации Абонентских пунктов	
2 (два)	
8. Наименование Абонентских пунктов (не более 47 символов включая пробелы)	
МУЗ Городская поликлиника 1234 – 1 *МУЗ Городская поликлиника 1234 – 2*	
9. ФИО Абонента зарегистрированного на Абонентском пункте	
МУЗ Городская поликлиника 1234 – 1: Иванов Иван Иванович *МУЗ Городская поликлиника 1234 – 2: Жукова Ирина Анатольевна*	
10. ФИО Локального администратора	
Иванов Иван Иванович	
11. Контактные телефоны Локального администратора	
(8 815) 22-22-22	
12.Контактный E-mail Локального администратора	
ivanovii@mail.ru	

13. Направления связи для организации защищённого обмена информацией:			
СМО «Капитал»; *СМО «Альфа-МС»;* *МУЗ Мурманский областной информационно-аналитический центр;* *Мурманский городской филиал ТФОМС Мурманской области;* *Комитет по здравоохранению г.Мурманск;*			
14. Перечень информационных систем, к которым необходим доступ:			
Единый регистр застрахованных по Мурманской области (Владелец ТФОМС Мурманской области)			
Дата заполнения заявки		*Подпись руководителя*	*М.П.*

ОБРАЗЕЦ

Приложение №3
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«ГОРОДСКАЯ ПОЛИКЛИНИКА №1234»
Г.МУРМАНСК

П Р И К А З

«___» _____2011 г. **№____**

О назначении Локального администратора МУЗ «Городская поликлиника №1234» г.Мурманск.

Для осуществления мер по пресечению несанкционированного доступа, администрирования и обеспечения бесперебойной работы информационных систем и Абонентских пунктов, принадлежащих МУЗ «Городская поликлиника №1234» г.Мурманск и относящихся к защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области.

ПРИКАЗЫВАЮ:

1. Назначить Локальным администратором МУЗ «Городская поликлиника №1234» г.Мурманск:

Иванова Ивана Ивановича - инженера АСУ МУЗ «Городская поликлиника №1234».

2. В своей работе по выполнению функций Локального администратора МУЗ «Городская поликлиника №1234» г.Мурманск руководствоваться:

- Положением о Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;
- Регламентом Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;
- Регламентом Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;

3. Контроль за исполнением приказа оставляю за собой.

Главный врач _____/П.П.Петров /

ОБРАЗЕЦ

Приложение №4
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«ГОРОДСКАЯ ПОЛИКЛИНИКА №1234»
Г.МУРМАНСК

П Р И К А З

«___» _____2011 г. **№____**

О назначении Абонентов Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области.

Для выполнения служебных обязанностей с использованием сервисов и информационных систем Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области:

ПРИКАЗЫВАЮ:

1. Назначить Абонентами Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области:

Иванова Ивана Ивановича - инженера АСУ МУЗ «Городская поликлиника №1234»

Жукову Ирину Анатольевну – медицинского статистика МУЗ «Городская поликлиника №1234»

2. В своей работе Абонентам Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области руководствоваться:

- Положением о Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;
- Регламентом Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;
- Регламентом Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;

3. Контроль за исполнением приказа оставляю за собой.

Главный врач _____/П.П.Петров /

ОБРАЗЕЦ

Приложение №5
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

Соглашение
о неразглашении персональных данных субъекта

Я, *Иванов Иван Иванович*, понимаю, что получаю доступ к персональным данным застрахованных лиц.

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

Я подтверждаю, что не имею права разглашать:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о состоянии здоровья;
- сведения о заработной плате;
- сведения о социальных льготах;
- сведения о занимаемой должности;
- сведения о наличии судимостей;
- адрес места жительства;
- домашний телефон;
- сведения о месте работы или учебы членов семьи и родственников;

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии с действующим законодательством.

"___"_____20__ г. _____

ОБРАЗЕЦ

Приложение №6
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

Доверенность
на получение дистрибутива ключей

(*наименование населенного пункта)* «_____»_____2011 г.

Муниципальное учреждение здравоохранения «Городская поликлиника №1234» в лице ***главного врача Петрова Петра Петровича*** уполномочивает:

Иванова Ивана Ивановича, паспорт ***4700 123456***, выданный ***Отделом УФМС России по Мурманской области в Первомайском АО г.Мурманска 23.03.2003 г.*** получить в Территориальном фонде обязательного медицинского страхования Мурманской области дистрибутив ключей для первичного запуска прикладной программы сети ViPNet.

Настоящая доверенность действительна по «___» _____ 20___г.

Подпись лица, получившего доверенность _____

Главный врач _____ /Петров П.П./

Приложение №7
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЖУРНАЛ УЧЁТА ВЫДАЧИ КЛЮЧЕВЫХ ДОКУМЕНТОВ

№ п/п	Дата выдачи	Организация	Ф.И.О. пользователя	Идентификатор дистрибутива	Тип носителя
1	2	3	4	5	6

Способ передачи (нарочным, лично в руки, письмом ДП (рег.номер) в адрес…)	Подпись получившего (отправившего по ДП)	Отметка об уничтожении
7	8	9

Приложение №8
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на изменение направлений связи и/или
предоставления доступа к информационным системам
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского страхования
Мурманской области.

	Директору Территориального фонда обязательного медицинского страхования Мурманской области Акульчеву В.А.
1. Полное наименование организации без сокращений (на основании учредительных документов)	
Муниципальное учреждение здравоохранения «Городская поликлиника №1234» г. Мурманск	
2. Сокращённое название организации	
МУЗ «Городская поликлиника №1234»	
3. Направления связи для организации защищённого обмена информацией:	
СМО «Капитал»; *СМО «Альфа-МС»;*	
4. Перечень информационных систем, к которым необходим доступ:	
Единый регистр застрахованных по Мурманской области (Владелец ТФОМС Мурманской области)	
5. Контактный телефон Локального администратора	
6. Контактный e-mail Локального администратора	

Дата заполнения заявки		*Подпись руководителя*	*М.П.*

Приложение №9
к Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ПРОТОКОЛ
установления межсетевого взаимодействия

«____» _____ 20__г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	**Наименование организаций**
№_____	*Полное наименование организации*
№_____	*Полное наименование организации*

2. Целью установление межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet сетей указанных организаций.
3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	**Должность**	**ФИО**
№_____		
№_____		

4. Передача начального и ответного экспорта между сетями №___ и №___ осуществлялась через специалиста, уполномоченного на данные действия.
5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети №___.
6. Для установления межсетевого взаимодействия были назначены серверы маршрутизаторы для организации шлюза:
   в сети №___ - «_____»
   в сети №___ - «_____»
7. При установлении межсетевого взаимодействия в части ЭЦП, были произведены импорты справочников ЭЦП главных абонентов сети №___ и №___.
8. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чём администраторы защищённых сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Делова почта] с указанием производимых изменений.
9. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищённых сетей, могущих привести к нарушению межсетевого взаимодействия.

Администратор сети ViPNet №_____	Администратор сети ViPNet №_____
_____ (ФИО)	_____ (ФИО)
_____ (подпись)	_____ (подпись)
«_____»_____20___г.	«_____»_____20___г.
М.П.	М.П.

Приложение №10
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЖУРНАЛ ИЗМЕНЕНИЙ

Территориального фонда обязательного медицинского страхования Мурманской области по организации межведомственного защищённого информационного взаимодействия с

_____

(полное наименование организации)

№ п/п	Наименование произведённого изменения в межсетевом взаимодействии	Дата изменения	Подпись специалиста, проводившего изменения
1.			
2.			
3.			
4.			

Пояснение по ведению журнала изменений.

В журнал заносятся все события, которые относятся к организации межведомственного защищённого информационного взаимодействия
- установление межсетевого взаимодействия;
- выбор Координатора, выполняющего функции сервер-шлюза;
-формирование межсетевого мастер-ключа;
-плановая смена межсетевого мастер-ключа;
-смена ключей при компрометации;
-модификация межсетевого взаимодействия (добавление или удаление сетевого узла и т.д.)

Каждая запись журнала должна заверяться специалистом, проводившим изменение.

ОБРАЗЕЦ

Приложение №11
К Регламенту Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на изменение Локального администратора и/или
зарегистрированных Абонентов
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского страхования
Мурманской области

	Директору Территориального фонда обязательного медицинского страхования Мурманской области Акульчеву В.А.
1. Полное наименование организации без сокращений (на основании учредительных документов)	
Муниципальное учреждение здравоохранения «Городская поликлиника №1234» г. Мурманск	
2. Сокращённое название организации	
МУЗ «Городская поликлиника №1234»	
3. ФИО Абонента зарегистрированного на Абонентском пункте	
МУЗ Городская поликлиника 1234 – 1: Платонова Ирина Викторовна *МУЗ Городская поликлиника 1234 – 2: Жукова Ирина Анатольевна*	
4. ФИО Локального администратора	
Наумов Николай Николаевич	
5. Контактные телефоны Локального администратора	
(8 815) 22-22-22	
6.Контактный E-mail Локального администратора	
naum@mail.ru	

Дата заполнения заявки		*Подпись руководителя*	*М.П.*