Приложение 2

к приказу ТФОМС Санкт-Петербурга

от 22 декабря 2014 г. № 520-А

РЕГЛАМЕНТ
ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ VIPNET
ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ
«ТЕРРИТОРИАЛЬНЫЙ ФОНД ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ САНКТ-ПЕТЕРБУРГА»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В целях настоящего Положения используются термины и определения в значениях, указанных в Положении о защищенной виртуально сети VipNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Положение о защищенной виртуальной сети ViPNet ТФОМС Санкт-Петербурга (далее - Положение) разработано 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 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Регламент определяет и устанавливает:

- порядок организации и подключения Участников к Защищенной сети ТФОМС Санкт-Петербурга;
- порядок предоставления доступа к информационным системам Защищенной сети;
- порядок организации защищенного межсетевого взаимодействия;
- порядок разрешения конфликтных ситуаций.

3. ПОРЯДОК ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ УЧАСТНИКОВ К ЗАЩИЩЕННОЙ СЕТИ

3.1 Организация подключения Участников к Защищенной 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 Защищенной сети (далее - Претендент) направляет в адрес ТФОМС Санкт-Петербурга заявление о намерении подключиться к Защищенной сети (Приложение №1).

3.2.1 В заявлении должна содержаться следующая информация:

- предполагаемое количество подключаемых Абонентских пунктов;
- общий перечень Участников, с которыми необходима организация защищенного 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 Санкт-Петербурга в течение 10-и рабочих дней со дня получения заявления о намерении подключиться к Защищенной сети, проводит оценку оснований

для подключения Претендента к Защищенной 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 Защищенной сети, не является основанием и гарантией подключения Претендента к Защищенной сети.

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

3.3.4 ТФОМС Санкт-Петербурга имеет право отказать Претенденту в подключении к Защищенной сети, объяснив причину отказа. Решение об отказе в подключении Претендента к Защищенной сети направляется в письменной форме в адрес Претендента в течение 5-и рабочих дней со дня принятия указанного решения.

3.3.5 ТФОМС Санкт-Петербурга уведомляет Претендента о принятии решения о подключении (отказе в подключении) к Защищенной сети, посредством электронной почты, указанной в заявление о намерении подключиться к Защищенной 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 Защищенной сети, Претендент самостоятельно приобретает программное обеспечение ViPNet [Клиент] и дистрибутив.

3.4.2 При оформлении договорных отношений по приобретению программного обеспечения ViPNet [Клиент] Претендент указывает номер Защищенной сети для подключения – 2001.

3.4.3 Подключение Претендента к Защищенной сети осуществляется ТФОМС Санкт-Петербурга, только после получения регистрационных файлов от производителя программного обеспечения или представителя производителя программного обеспечения.

3.4.4 ТФОМС Санкт-Петербурга 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 Санкт-Петербурга заявку на подключение (Приложение №2).

3.5.2 В течение 3 рабочих дней со дня получения от Претендента заявки на подключение ТФОМС Санкт-Петербурга:

- 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;
- по завершению обозначенных работ уведомляет об этом Претендента.

3.5.3 Формирование дистрибутива ключей для Абонентских пунктов вместе с паролем доступа к нему производится в присутствии Претендента на рабочем месте Корпоративной информационной системы ТФОМС Санкт-Петербурга, аттестованной в соответствии с требованиями по безопасности персональных данных.

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

а) Предоставить в адрес ТФОМС Санкт-Петербурга:

- копию приказа о назначении Локального администратора (Приложение №3) и Абонентов Защищенной сети (Приложение №4);
- копии соглашений с Локальным администратором и Абонентами Защищенной сети о неразглашении информации, к которой будет получен доступ в связи с выполнением своих функций (Приложение №5);

б) Направить в ТФОМС Санкт-Петербурга 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).

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

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

4.3 Рассмотрение заявки.

4.3.1 ТФОМС Санкт-Петербурга в течение 5-ти рабочих дней со дня получения рассматривает заявку, проводит оценку технической возможности для изменения направлений связи и/или организации доступа к информационным системам Защищенной сети.

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

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

4.3.4 ТФОМС Санкт-Петербурга уведомляет Претендента об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, посредством электронной почты, со ссылкой на соответствующее Решение.

4.3.5 Формирование и передача ключевой информации

4.3.6 В течение 5 рабочих дней со дня уведомления Участника о принятии решения об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети ТФОМС Санкт-Петербурга:

- 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.

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

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

4.3.9 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 Защищенной сетью и сторонней сетью ViPNet, Координатор Защищенной 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 Санкт-Петербурга 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 Санкт-Петербурга имеет право отказать в организации межсетевого взаимодействия, объяснив причину отказа.

5.3.3 В случае принятия решения об организации межсетевого взаимодействия ТФОМС Санкт-Петербурга 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 Защищенной 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 Защищенной 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. КОМПРОМЕТАЦИЯ КЛЮЧЕЙ

7.1. 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).

7.2. 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.

7.3. 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.

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

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

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

7.7. 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.

7.8. Локальный администратор доводит информацию о факте компрометации (или предполагаемом факте компрометации) до Г лавного администратора.

7.9. 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 Защищенной сети.

8. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

8.1. Компрометация ключей Абонента.

При наступлении любого из перечисленных в п. 7.1 настоящего Регламента событий Абонент, должен немедленно прекратить работу на своём Абонентском пункте и сообщить о факте компрометации администратору своей сети ViPNet.

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

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

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

8.2. Внеплановая смена межсетевого мастер-ключа.

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

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

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

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

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

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

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

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

Приложение №1
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Директору
Государственного учреждения
«Территориальный фонд обязательного
медицинского страхования Санкт-Петербурга»
Кужелю А.М.

О подключении
к защищенной виртуальной сети VipNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Сакнт-Петербурга»

Прошу подключить СПб ГБУЗ «Городская поликлиника № » г. Санкт-Петербург *к защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» для обмена информацией в сфере обязательного медицинского страхования Санкт-Петербурга, содержащей персональные данные.*

Планируемое число подключаемых абонентских пунктов - *1* (один).

Перечень информационных систем, к которым необходим доступ: Единая информационная система обязательного медицинского страхования Санкт-Петербурга (ЕИС ОМС).

Лицо, ответственное за подключение, и контактный телефон: Иванов Иван Иванович, (812) 111-22-33, адрес электронной почты.

Руководитель организации _____ /ФИО/

М.П.

Приложение №2
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Заявка
на подключение к Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Директору
Государственного учреждения
«Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»
Кужелю А.М.

1. Полное наименование организации без сокращений (на основании учредительных документов)
СПб ГБУЗ «Городская поликлиника №___» *г. Санкт-Петербург*
2. Сокращенное название организации
СПб ГБУЗ «Городская поликлиника №___»
3. Юридический адрес организации с индексом
г. Санкт-Петербург, Невский пр. 1, 196600
4. Фактический (почтовый) адрес организации с индексом
г. Санкт-Петербург, Невский пр. 1, 196600
5. ФИО руководителя
Петров Пётр Петрович
6. Должность руководителя
Главный врач
7. Количество необходимых для регистрации Абонентских пунктов
1(один)
8. Наименование Абонентских пунктов(не более 47 символов включая пробелы)
Городская поликлиника ____ Client 1
9. ФИО Абонента зарегистрированного на Абонентском пункте
Иванов Иван Иванович
10. Контактные телефоны Локального администратора
(812)111-22-33
11. Контактный E-mail Локального администратора
iivanov@mail.ru
12. Направление связи для организации защищенного обмена информацией:
ЗАО «СК «АВЕСТА-Мед» *ЗАО «СМК АСК-Мед»* *Государственное учреждение «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»*
13. Перечень информационных систем, к которым необходим доступ:
Единая информационная система обязательного медицинского страхования Санкт-Петербурга(ЕИС ОМС).

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

Приложение №3
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

СПБ ГБУЗ
«ГОРОДСКАЯ ПОЛИКЛИНИКА №__»
Г. САНКТ-ПЕТЕРБУРГ
ПРИКАЗ

«___» _____ 2014 г. **№ ___**

О назначении Локального администратора СПб ГБУЗ «Городская поликлиника №____» г. Санкт-Петербург.

Для осуществления мер по пресечению несанкционированного доступа, администрирования и обеспечения бесперебойной работы информационных систем и Абонентских пунктов, принадлежащих СПб ГБУЗ «Городская поликлиника №____» г. Санкт-Петербург и относящихся к защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга».

ПРИКАЗЫВАЮ:

1. Назначить Локальным администратором СПБ ГБУЗ «Городская поликлиника №____» г. Санкт-Петербург:
   - Иванова Ивана Ивановича - инженера СПБ ГБУЗ «Городская поликлиника №____».
2. В своей работе по выполнению функций Локального администратора СПБ ГБУЗ «Городская поликлиника №____» г. Санкт-Петербург руководствоваться:
   - Положением о Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»;
   - Регламентом Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»;
3. Контроль за исполнением приказа оставляю за собой.

Главный врач _____ /_____/

Приложение №4
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

СПБ ГБУЗ «ГОРОДСКАЯ ПОЛИКЛИНИКА №___»
Г. САНКТ-ПЕТЕРБУРГ
ПРИКАЗ

«___» _____ 2014 г. **№ ___**

О назначении Абонентов Защищенной виртуальной сети VipNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга».

Для выполнения служебных обязанностей с использованием сервисов и информационных систем Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»:

ПРИКАЗЫВАЮ:

1. Назначить Абонентами Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»:
   - _____
2. В своей работе Абонентам Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» руководствоваться:

- Положением о Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»;
- Регламентом Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»;

3. Контроль за исполнением приказа оставляю за собой.

Главный врач _____ /_____/

Приложение №5
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Соглашение
О неразглашении персональных данных субъекта

Я, _____, паспорт серия _____, номер _____, выданный _____ « ___ » _____ _____ года, в период трудовых отношений с ГУЗ Городская поликлиника №___ г. Санкт-Петербурга и после их прекращения в соответствии с законодательством Российской Федерации в сфере защиты персональных данных, обязуюсь:

1) не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения ответственного за обработку данных в организации;

2) выполнять требования приказов, положения и инструкций по обработке персональных данных в части меня касающейся;

3) в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за обработку персональных данных;

4) не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых и обрабатываемых в защищенной сети.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных при автоматизированной обработке информации, а также при обработке информации без использования средств автоматизации.

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

11.01.2014 г. _____/_____/

Приложение №6
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Доверенность на получение дистрибутива ключей

г. Санкт-Петербург « ____» _____ 2014 г.

СПб ГБУЗ «Городская поликлиника №_» в лице Главного врача _____ уполномочивает:

_____, паспорт _____, выданный _____ ***(дата выдачи)*** получить в государственном учреждении «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» дистрибутив ключей для первичного запуска прикладной программы сети ViPNet.

Настоящая доверенность действительна по «__ » _____ 20___ г.

Подпись лица, получившего доверенность _____

Главный врач _____ /_____/

Приложение №7
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

№ п/п	Дата выдачи	Организация	Ф.И.О. пользователя	Идентификатор дистрибутива	Тип носителя	Способ передачи (нарочным, лично в руки, письмом ДП (рег.номер) в адрес...)	Подпись получившего (отправившего по ДП)	Отметка об уничтожении
1	2	3	4	5	6	7	8	9

Приложение №8
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Заявка
на изменение направлений связи и/или предоставление доступа к информационным ресурсам Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Директору
Государственного учреждения
«Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»
Кужелю А.М.

1. Полное наименование организации без сокращений (на основании учредительных документов)
СПб ГБУЗ «Городская поликлиника №__» *г. Санкт-Петербурга*
2. Сокращенное название организации
СПБ ГБУЗ «Городская поликлиника №__»
3. Наименование Абонентских пунктов(не более 47 символов включая пробелы)
СПБ ГБУЗ Городская поликлиника ___ Client 1
4. Контактные телефоны Локального администратора
(812)111-22-33
5. Контактный E-mail Локального администратора
iivanov@mail.ru
6. Направление связи для организации защищенного обмена информацией:
ЗАО «СК «АВЕСТА-Мед» *ЗАО «СМК АСК-Мед»* *Государственное учреждение «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»*
7. Перечень информационных систем, к которым необходим доступ:
Единая информационная система обязательного медицинского страхования Санкт-Петербурга(ЕИС ОМС).

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

Приложение №9
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Протокол установления межсетевого взаимодействия

« ____» _____ 2014 г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	**Наименование организаций**
№ 2001	*Государственное учреждение «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»*
№	*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**
№ 2001		
№		

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 защищенных 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 защищенных сетей, могущих привести к нарушению межсетевого взаимодействия.

Администратор сети №

(ФИО)

(подпись)

«___» _____ 2014 г.
М.П.

Администратор сети №

(ФИО)

(подпись)

«___» _____ 2014 г.
М.П.

Приложение №10
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

ЖУРНАЛ ИЗМЕНЕНИЙ

Государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» по организации межведомственного защищенного информационного взаимодействия с

_____

(полное название 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 защищенного информационного взаимодействия:

- установление межсетевого взаимодействия;
- выбор Координатора, выполняющего функции сервера – 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.

Приложение №11
К Регламенту Защищенной виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Заявка
на изменение Локального администратора и/или зарегистрированных абонентов Защищенной виртуальной сети ViPNet
государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»

Директору
Государственного учреждения
«Территориальный фонд обязательного медицинского страхования Санкт-Петербурга»
Кужелю А.М.

1. Полное наименование организации без сокращений (на основании учредительных документов)
СПб ГБУЗ «Городская поликлиника №__» *г. Санкт-Петербурга*
2. Сокращенное название организации
СПБ ГБУЗ «Городская поликлиника №__»
3. ФИО Абонента зарегистрированного на Абонентском пункте
СПБ ГБУЗ Городская поликлиника _____ Client 1 – Иванов Иван Иванович
4. ФИО Локального администратора
Иванов Иван Иванович
5. Контактные телефоны Локального администратора
(812)111-22-33
6. Контактный E-mail Локального администратора
iivanov@mail.ru

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