Приложение 3

к приказу ТФОМС Санкт-Петербурга

от 22 декабря 2014 г. № 520-А

РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ 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. Регламент устанавливает общий порядок и условия предоставления Удостоверяющим центром корпоративного уровня Защищённой сети ТФОМС Санкт-Петербурга Участникам возможности участвовать в обмене электронными документами с применением электронной подписи.

2.2. Присоединение к Регламенту УЦ, производится путем заключения Участниками Соглашения о защищенном обмене электронными документами (далее - Соглашение) (Приложение №1).

2.3. Участник имеет право в одностороннем порядке расторгнуть Соглашение, письменно уведомив об этом ТФОМС Санкт-Петербурга за 30 календарных дней, до дня расторжения.

2.4. Уведомление о расторжении Соглашения, полученное ТФОМС Санкт-Петербурга от Участника, является основанием для обязательного аннулирования сертификатов ключей проверки электронных подписей Пользователей Удостоверяющего центра (далее - Пользователей УЦ), уполномоченных данным Участником. Датой аннулирования, указанных сертификатов ключей проверки электронных подписей Пользователя УЦ будет дата расторжения Соглашения.

3. НАЗНАЧЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

3.1 Удостоверяющий центр предназначен для обеспечения:

- аутентификации Участников в процессе взаимодействия;
- возможности использования электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия Участников;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия Участников;

3.2 В процессе своей деятельности Удостоверяющий центр:

- вносит в реестр Удостоверяющего центра регистрационную информацию о Пользователях УЦ;
- формирует и обновляет справочно-ключевую информацию для организации защищённого обмена информацией в рамках Защищённой сети;
- создает сертификаты ключей проверки электронных подписей;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей;
- ведет реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей;
- создает ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

- осуществляет по обращениям Пользователей УЦ проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

3.3 Все электронные подписи созданные в Удостоверяющем центре являются усиленными неквалифицированными электронными подписями.

3.4 Выполнение своих функций Удостоверяющий центр осуществляет на безвозмездной основе.

4. ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА, ИЗГОТОВЛЕНИЕ И УПРАВЛЕНИЕ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

4.1. Пользователями УЦ называются лица, зарегистрированные в Удостоверяющем центре и осуществляющие обмен электронными документами в рамках заключённого Соглашения.

4.2. Проходить процедуру регистрации в Удостоверяющем центре, либо быть зарегистрированным Пользователем УЦ, может только физическое лицо, представляющее юридическое лицо.

4.3. Порядок регистрации, изготовления и управления сертификатами ключей проверки электронной подписи Пользователей УЦ.

4.3.1. Регистрация Пользователей УЦ состоит из 3-х последовательных этапов:
- подключение Участника к Защищённой сети;
- присоединение к Регламенту УЦ;
- регистрация и изготовление сертификата ключа проверки электронной подписи Пользователя УЦ;

4.3.2. Подключение к Защищённой сети, осуществляется согласно разделу 3 Регламента Защищённой виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга».

4.3.3. Присоединение к Регламенту УЦ производится путём заключения Участником Соглашения о защищённом обмене электронными документами (Приложение №1).

4.3.4. Регистрация и изготовление сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется после предоставления в адрес ТФОМС Санкт-Петербурга:
- подписанного директором ТФОМС Санкт-Петербурга и руководителем Участника Соглашение об организации защищенного обмена электронными документами;
- заявления на регистрацию Пользователя УЦ (Приложение №3);
- заявление на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ (Приложение №4);
- доверенности на предоставление заявительных документов и получение подписей и сертификата Пользователя УЦ.

4.3.5. После предоставления заявлений на регистрацию и изготовление сертификата ключа проверки электронной подписи Уполномоченное лицо в течение 1 (одного) рабочего дня, осуществляет её рассмотрение и обработку.

4.3.6. В случае отказа в регистрации и изготовлении сертификата ключа проверки электронной подписи Уполномоченное лицо письменно уведомляет об этом руководителя Участника.

4.3.7. В случае принятия положительного решения Уполномоченное лицо осуществляет регистрацию Пользователя УЦ, генерацию ключевой информации, изготовление сертификата ключа проверки электронной подписи и распечатывает сертификат ключа проверки электронной подписи в двух экземплярах.

4.3.8. Два экземпляра сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе визируются Уполномоченным лицом и заверяются печатью.

4.3.9. После изготовления сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет об этом Пользователя УЦ, после чего Пользователь УЦ должен лично или через Локального администратора Участника, получить сформированные ключевые документы у Уполномоченного лица.

4.3.10. Локальный администратор Участника для получения к сформированного ключевого носителя, содержащего ключ электронной подписи и сертификат ключа проверки электронной подписи Пользователя УЦ должен представить в Удостоверяющий центр доверенность на право подписи и получения сертификата ключа проверки электронной подписи за Пользователя УЦ и получения сформированной ключевой информации (Приложение №5), а также документы, определённые Соглашением «Об организации защищённого обмена электронными документами» - Пользователя УЦ.

Представитель наделяется правом расписываться в сертификате ключа проверки электронной подписи на бумажном носителе и в соответствующих документах Удостоверяющего центра для исполнения поручений, определённых доверенностью.

4.3.11. Изготовленные ключи записываются на отчуждаемый машинный носитель, предоставляемый Пользователем УЦ.

4.3.12. Ключевой носитель должен удовлетворять следующим требованиям:

- быть отформатированным;
- не содержать никакой информации;

4.3.13. Ключевые носители, не удовлетворяющие требованиям п. 5.3.12, для записи ключевой информации не принимаются.

4.3.14. Факт выдачи ключей заносится в Журнал учёта выдачи ключевых документов под роспись владельца или Локального администратора.

4.3.15. После получения всей необходимой ключевой информации и сертификата ключа проверки электронной подписи Локальный администратор вводит полученные данные на Абонентском пункте Защищённой сети, на котором зарегистрирован Пользователь УЦ.

4.4. Аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется по заявлению на отзыв сертификата ключа проверки электронной подписи руководителем Участника (Приложение №6).

4.4.1. Заявление на отзыв сертификата ключа проверки электронной подписи в бумажной форме подаётся Пользователем УЦ лично.

4.4.2. Срок рассмотрения заявления на отзыв сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

4.4.3. Заявление на отзыв сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя УЦ.

4.4.4. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер отзываемого сертификата;
- причину отзыва сертификата;
- дату и подпись заявителя.

4.5. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется по заявлению на приостановление действия

сертификата ключа проверки электронной подписи руководителем Участника (Приложение №6).

4.5.1. Заявление на приостановление действия сертификата ключа проверки электронной подписи в бумажной форме подаётся Пользователем УЦ лично.

4.5.2. Срок рассмотрения заявления на приостановление сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

4.5.3. Заявление на приостановление сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя УЦ. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого приостанавливается;
- причину приостановления действия сертификата;
- срок, на который приостанавливается действие сертификата;
- дату и подпись заявителя.

4.6. Возобновление действия сертификата ключа проверки электронной подписи Пользователя УЦ, осуществляется по заявлению на возобновление действия сертификата ключа проверки электронной подписи руководителем Участника (Приложение №6).

4.6.1. Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме подаётся Пользователем УЦ лично.

4.6.2. Срок рассмотрения заявления на возобновление сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

4.6.3. Заявление на возобновление сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя УЦ. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого возобновляется;
- причину возобновления действия сертификата;
- дату и подпись заявителя.

4.7. Хранение сертификата ключа проверки электронной подписи Пользователей УЦ в реестре выданных и аннулированных сертификатов ключей проверки электронной подписи Удостоверяющего центра, осуществляется в течение установленного срока действия сертификата ключа проверки электронной подписи.

4.8. Срок архивного хранения сертификата ключа проверки электронной подписи устанавливается в соответствии со сроком, определённым разделом 10 Регламента УЦ.

4.9. Порядок ведения реестра сертификатов, осуществляется в соответствии с Руководством администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр].

5. ОРГАНИЗАЦИЯ ЗАЩИЩЁННОГО ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ МЕЖДУ СТОРОНАМИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕДУР МЕЖСЕТЕВОГО ОБМЕНА СЕТЕЙ VIPNET

5.1. Организация межсетевого взаимодействия осуществляется согласно разделу 5 Регламента Защищённой виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга».

5.2. В случае организации защищённого обмена электронными документами с использованием процедур межсетевого обмена сетей ViPNet, между ТФОМС Санкт-Петербурга и доверенной сетью ViPNet заключается Соглашения о защищённом обмене электронными документами.

5.3. Для проверки сертификатов ключей проверки электронной подписи доверенных сетей ViPNet, приславших подписанную информацию, используются сертификаты Администраторов доверенных сетей ViPNet

5.4. Обмен сертификатами Администраторов сетей ViPNet осуществляется согласно Руководству администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр].

6. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УЦ

6.1. Срок действия ключа электронной подписи и ключа проверки электронной подписи Уполномоченного лица составляет 2 года.

6.2. Начало периода действия ключа электронной подписи Уполномоченного лица исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

6.3. Максимальный срок, который может быть установлен в качестве срока действия сертификата ключа проверки электронной подписи Уполномоченного лица, составляет 5 лет.

7. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

7.1. Срок действия ключа электронной подписи Пользователя УЦ, соответствующего сертификату ключа проверки электронной подписи, владельцем которого он является, составляет 12 месяцев.

7.2. Начало периода действия ключа электронной подписи Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи Пользователя УЦ.

7.3. Срок действия ключа электронной подписи устанавливается равным сроку действия сертификата ключа проверки электронной подписи.

7.4. Максимальный срок, который может быть установлен в качестве срока действия сертификатов ключей проверки электронной подписи Пользователей УЦ, составляет 1 год.

7.5. Срок действия сертификата ключа проверки электронной подписи устанавливается УЦ в момент его изготовления.

8. АРХИВНОЕ ХРАНЕНИЕ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

8.1. Архивированию подлежит следующая информация:

- реестр выданных и аннулированных сертификатов ключей проверки электронных подписей Пользователей УЦ;
- сертификаты ключей проверки электронных подписей Уполномоченного лица УЦ;
- реестр зарегистрированных Пользователей УЦ;
- заявления на изготовление ключей Пользователей УЦ;
- заявление на аннулирование (отзыв) сертификатов ключей проверки электронных подписей Пользователей УЦ;
- заявление на приостановление действия сертификатов ключей проверки

электронных подписей Пользователей УЦ;

- заявление на возобновление действия сертификатов ключей проверки электронных подписей Пользователей УЦ;
- служебные документы УЦ.

8.2. Информация, внесенная в реестр выданных и аннулированных сертификатов ключей проверки электронных подписей, подлежит хранению в течение всего срока деятельности Удостоверяющего центра.

8.3. Выделение архивных документов к уничтожению и уничтожение осуществляется в соответствии с инструкцией по общему делопроизводству.

9. УПРАВЛЕНИЕ КЛЮЧАМИ

9.1. Плановая смена ключей Уполномоченного лица.

9.1.1. Плановая смена ключей Уполномоченного лица выполняется в соответствии со сроком действия сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего Центра.

9.1.2. Процедура плановой смены ключей Уполномоченного лица осуществляется в следующем порядке:

- Уполномоченное лицо формирует новый ключ электронной подписи;
- Уполномоченное лицо изготавливает сертификат нового ключа проверки электронной подписи и подписывает его электронной подписью с использованием нового ключа электронной подписи.

9.2. Внеплановая смена ключей Уполномоченного лица.

9.2.1. Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Уполномоченного лица.

9.2.2. При компрометации ключей шифрования Уполномоченного лица прекращается работа по их использованию.

9.2.3. Процедура внеплановой смены ключей электронной подписи Уполномоченного лица выполняется после получения уведомления о компрометации ключа электронной подписи. В течение одного рабочего дня:

- аннулируется сертификат ключа проверки электронной подписи Уполномоченного лица ключа электронной подписи;
- ключи Уполномоченного лица объявляются скомпрометированными;
- производится рассылка сформированных обновлений ключей на узлы Защищённой сети.

9.2.4. После выполнения процедуры внеплановой смены ключей Уполномоченного лица, сертификат ключа проверки электронной подписи Уполномоченного лица аннулируется (отзывается) путём занесения в список отозванных сертификатов.

9.3. Плановая смена ключей Пользователей.

9.3.1. Плановая смена ключей электронной подписи Пользователя УЦ выполняется в соответствии со сроком действия сертификата ключа проверки электронной подписи Пользователя УЦ.

9.3.2. Процедура плановой смены ключей Пользователей УЦ осуществляется в следующем порядке:

- Уполномоченное лицо формирует новый ключ электронной подписи;
- Уполномоченное лицо изготавливает сертификат нового ключа проверки электронной подписи и подписывает его электронной подписью.

9.4. Внеплановая смена ключей Пользователей УЦ.

9.4.1. Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа Пользователя УЦ.

9.4.2. В случае компрометации только ключей электронной подписи Пользователь УЦ обязан немедленно сообщить об этом своему Локальному администратору и не использовать эти ключи для подписи документов. При компрометации ключей шифрования Пользователь УЦ обязан прекратить работу на своём Абонентском пункте.

9.4.3. Ключи пользователя могут считаться скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным файл ключевого дистрибутива;
- посторонним лицам мог стать доступным съёмный носитель с ключевой информацией;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере;

9.4.4. Процедура внеплановой смены ключей Пользователей УЦ выполняется Уполномоченным лицом.

9.4.5. Уполномоченное лицо после получения уведомления о компрометации ключа электронной подписи в течение одного рабочего дня:

- аннулирует сертификат ключа проверки электронной подписи;
- объявляет ключи данного Пользователя УЦ скомпрометированными;

Производит рассылку сформированных обновлений ключей на Абонентские пункты сети.

9.5. После выполнения процедуры внеплановой смены ключей Пользователя УЦ, сертификат ключа проверки электронной подписи Пользователя УЦ аннулируется (отзывается) путём занесения в список отозванных сертификатов.

10. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

10.1. Удостоверяющий центр издаёт сертификаты ключей проверки электронной подписи Пользователей УЦ и Уполномоченного лица УЦ в электронной форме (далее – Сертификаты открытых ключей) формата X.509 версии 3.

10.2. Удостоверяющий центр издаёт списки отозванных сертификатов ключей проверки электронной подписи Пользователей УЦ и Уполномоченного лица УЦ в электронной форме (далее – Сертификаты открытых ключей) формата X.509.

Приложение №1
К Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
государственного учреждения
«Территориальный фонд обязательного медицинского
страхования Санкт-Петербурга»

СОГЛАШЕНИЕ
об организации защищенного обмена электронными документами

г. Санкт-Петербург « » _____ 2014 г.

Государственное учреждение «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга, в лице директора _____, действующего на основании _____, именуемый в дальнейшем ТФОМС Санкт-Петербурга, и_____ _____, именуемый в дальнейшем Организация, в лице _____, действующего на основании _____, вместе именуемые «Стороны» на основании Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи», в целях организации защищённого обмена электронными документами в рамках Защищённой виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга, заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В силу настоящего Соглашения Организация присоединяется к Регламенту удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» (далее – Регламент УЦ), утвержденному приказом директора ТФОМС Санкт-Петербурга.

1.2. Организация, присоединившаяся к Регламенту УЦ, осуществляет обмен документами в электронном виде с использованием программных продуктов, объединённых под торговой маркой ViPNet, обеспечивающих создание защищённой виртуальной сети с возможностью использования электронной подписи на базе общедоступной сети Интернет.

2. ПРАВА И ОЯЗАННОСТИ СТОРОН

2.1. Стороны признают, что используемые при электронном обмене средства защиты, обеспечивающие защиту от несанкционированного доступа через каналы связи, шифрование и электронную подпись, достаточны для обеспечения конфиденциальности информационного взаимодействия сторон.

2.2. Стороны обязуются:

2.2.1. При проведении защищённого обмена электронными документами руководствоваться законодательством Российской Федерации, Регламентом УЦ,

Положением о виртуальной Защищённой сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга», Регламентом виртуальной Защищённой сети ViPNet государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга», настоящим Соглашением и документацией на программные средства ViPNet.

2.2.2. Обеспечивать целостность прикладного и системного программного обеспечения на рабочем месте Стороны и отсутствие в программной среде злонамеренного программного кода.

2.2.3. Не вносить исправления, изменения или дополнения, а также не передавать третьим лицам средства электронной подписи, программное обеспечение и соответствующую техническую документацию.

2.2.4. Содержать в исправном состоянии компьютеры, участвующие в электронном взаимодействии, принимать организационные и технические меры для предотвращения несанкционированного доступа к данным компьютерам, установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены, не допускать появления на взаимодействующих компьютерах компьютерных вирусов.

2.2.5. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Соглашению, должна о наступлении и прекращении обстоятельств препятствующих исполнению обязательств, немедленно извещать другую сторону.

2.3. ТФОМС Санкт-Петербурга имеет право:

2.3.1. Отказывать Участнику в приёме/передаче электронных документов с указанием причины отказа.

2.3.2. Приостанавливать обмен электронными документами при:

- несоблюдении Участником требований к приёму/передаче электронных документов и обеспечению информационной безопасности, предусмотренных законодательством Российской Федерации и условиями настоящего Соглашения;
- разрешении спорных ситуаций, а также для выполнения неотложных, аварийных и ремонтно-восстановительных работ на АРМ Стороны с уведомлением других Участников о сроках проведения этих работ.

2.3.3. Требовать от других Участников приостановления обработки всех электронных документов в случаях компрометации ключей электронной подписи.

3. ТЕХНИЧЕСКИЕ УСЛОВИЯ

3.1. Стороны за свой счёт приобретают, устанавливают и обеспечивают работоспособность средств защиты информации и электронной подписи, обеспечивающих подключение и функционирование в Защищённой сети.

3.2. Стороны оплачивают средства связи и каналы связи, необходимые для работы в Защищённой сети.

3.3. Выдача сертификатов ключей проверки электронной подписи осуществляется ТФОМС Санкт-Петербурга.

4. ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

4.1. Обмен электронными документами осуществляется по открытым каналам связи с использованием средств криптографической защиты информации и электронной подписи.

4.2. Обмен документами, их подпись и подтверждение целостности и подлинности осуществляется в соответствии с руководствами пользователей на технические средства и средства защиты, обеспечивающие такой обмен.

4.3. Отправленные и полученные электронные документы сохраняются и могут быть перенесены на любые носители.

4.4. Все подписанные электронные документы должны хранится в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров – до их разрешения.

4.5. Обязанности по организации архивов электронных документов возлагаются на каждую из Сторон, в части их касающейся.

4.6. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения.

4.7. Электронные документы, подписанные некорректными электронными подписями, в обработку не принимаются.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

5.2. Каждая из Сторон несёт ответственность за содержание всех принятых/переданных электронных документов, подписанных владельцем Сертификата ключа проверки электронной подписи Стороны.

5.3. Стороны не несут ответственность за возможные временные задержки исполнения и/или искажения электронного документа, возникающие по вине третьих лиц, предоставляющих услуги связи для работы Защищённой сети.

5.4. Сторона не несёт ответственность за убытки других Участников, возникшие вследствие несвоевременного сообщения соответствующего Участника о компрометации ключей электронной подписи.

5.5. Сторона не несёт ответственность за ущерб, возникший вследствие разглашения пользователем другого Участника собственного ключа электронной подписи, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

5.6. Сторона не несёт ответственность за неработоспособность оборудования и программных средств других Участников, повлекшую за собой невозможность доступа к Защищённой сети и возникшие в результате задержки в осуществлении передачи информации, а также за возможное уничтожение (в полном или частичном объёме) информации, содержащейся на вычислительных средствах других Участников.

5.7. Сторона полностью несёт ответственность за риски, связанные с подключением ее вычислительных средств к сети Интернет. Стороны самостоятельно обеспечивает защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет.

6. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

6.1. При возникновении конфликтных ситуаций, возникающих в ходе защищённого обмена электронными документами, Стороны разрешают их путём переговоров.

6.2. При недостижении согласия, споры разрешаются в соответствии с действующим законодательством.

7. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

7.1. По взаимному согласию Сторон в текст Соглашения могут вноситься изменения и дополнения.

7.2. Все изменения и дополнения к настоящему Соглашению имеют юридическую силу и являются действительными, если они составлены в письменном виде и подписаны Сторонами.

7.3. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

8. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

8.1. Настоящее Соглашение заключено на неопределённый срок.

8.2. Настоящее Соглашение вступает в силу и становится обязательным для Сторон с момента его заключения.

8.3. Изменения и дополнения к настоящему Соглашению оформляются в письменной форме и действительны с момента подписания Сторонами.

8.4. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чём необходимо письменно уведомить другую Сторону не позднее, чем за 30 календарных дней до дня его расторжения.

9. ЮРИДИЧЕСКИЕ АДРЕСА И ПОДПИСИ СТОРОН:

Организация:	Организация:
Наименование:	Наименование:
Адрес:	Адрес:
Тел./ Факс:	Тел./ Факс:
Директор	Директор
_____/ /	_____/ /
М.П.	М.П.

Приложение №2
К Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
государственного учреждения
«Территориальный фонд обязательного медицинского
страхования Санкт-Петербурга»

ЗАЯВКА

на изготовление, отзыв, приостановление действия, возобновление действия
нужное подчеркнуть

сертификатов ключей проверки электронных подписей работников

_____

(наименование подразделения)

Прошу сформировать ключи и изготовить сертификаты, отозвать
нужное подчеркнуть

сертификаты, приостановить действие сертификатов, возобновить действие
нужное подчеркнуть

сертификатов ключей проверки электронных подписей следующих работников

№ п/п	Фамилия Имя Отчество	Должность	Подпись работника
1			
2			
3			
4			

Руководитель подразделения _____/Фамилия И.О./

Приложение №3
К Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
государственного учреждения
«Территориальный фонд обязательного медицинского
страхования Санкт-Петербурга»

ЗАЯВЛЕНИЕ
на регистрацию Пользователя Удостоверяющего центра

_____

(Наименование Участника)

в лице, _____

(Должность Руководителя)

_____

(Фамилия, Имя, Отчество руководителя)

действующего на основании_____

Просит зарегистрировать уполномоченного представителя

_____

(Фамилия, Имя, Отчество)

в Реестре Удостоверяющего центра и наделить полномочиями Пользователя Удостоверяющего центра, установленными Соглашением от «____»_____20___г. №____ «Об организации защищённого обмена электронными документами».
Настоящим_____

(Фамилия, Имя, Отчество)

соглашается с обработкой своих персональных данных Удостоверяющим центром и признаёт, что персональные данные, заносимые в сертификаты ключей проверки электронных подписей, владельцами которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №4
К Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
государственного учреждения
«Территориальный фонд обязательного медицинского
страхования Санкт-Петербурга»

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра

_____

(Наименование Участника)

в лице, _____

(Должность Руководителя)

_____

(Фамилия, Имя, Отчество руководителя)

действующего на основании_____

Просит сформировать ключи электронной подписи, записать сформированный ключ электронной подписи на предоставленный ключевой носитель и изготовить сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

_____

(Фамилия, Имя, Отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)	Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Organization Unit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Contry (C)	RU	
Extended Key Usage	Проверка подлинности клиента Защищённая электронная почта	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4)

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №5
К Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
государственного учреждения
«Территориальный фонд обязательного медицинского
страхования Санкт-Петербурга»

ДОВЕРЕННОСТЬ
на предоставление заявительных документов и получение подписей и сертификата Пользователя Удостоверяющего центра
(образец оформления)

Совершено «_____»_____20___ г. в г._____

_____
(Наименование Участника)

в лице, _____
(Должность Руководителя)

_____
(Фамилия, Имя, Отчество руководителя)

действующего на основании_____
уполномачивает_____
(Фамилия, Имя, Отчество)

_____
(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Удостоверяющий центр необходимые документы, определённые Соглашением от «____»_____20___г. №____ «Об организации защищённого обмена электронными документами» - Пользователя Удостоверяющего центра

_____
(Ф.И.О. Пользователя Удостоверяющего центра)

2. Получить сформированный ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра _____
(Ф.И.О. Пользователя Удостоверяющего центра)

3. Расписываться в получении сертификате ключа проверки электронной подписи (на бумажном носителе) и в соответствующих документах Удостоверяющего центра для исполнения поручений, определённых настоящей доверенностью.

Срок действия настоящей доверенности «____»_____20___г.

Подпись _____ _____ подтверждаю.
(Фамилия И.О. уполномоченного лица) (подпись)

Пользователь Удостоверяющего центра _____/Фамилия И.О./

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника
М.П.

Приложение №6
К Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
государственного учреждения
«Территориальный фонд обязательного медицинского
страхования Санкт-Петербурга»

ЗАЯВЛЕНИЕ
на аннулирование (отзыв), на приостановление действия, на возобновление действия
нужное подчеркнуть

сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра

(Наименование Участника)

в лице, _____

(Должность Руководителя)

(Фамилия, Имя, Отчество руководителя)

действующего на основании_____

просит аннулировать (отозвать), приостановить действие, возобновить действие
нужное подчеркнуть

сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

(Фамилия, Имя, Отчество)

Содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата
CommonName (CN)	Фамилия, Имя, Отчество
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Субъект Федерации
Contry (C)	RU

Срок приостановления действия сертификата _____ дней.
заполняется при приостановлении сертификата

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.