Соглашение N \_\_\_

об электронном документообороте

|  |  |
| --- | --- |
| г. Москва | "\_\_"\_\_\_\_\_\_\_\_ \_\_\_\_ г. |

**Федеральное казенное учреждение «Федеральный центр планирования и организации лекарственного обеспечения граждан» Министерства здравоохранения Российской Федерации** в лице директора Максимкиной Елены Анатольевны, действующего на основании Устава, далее - Сторона 1, с одной стороны и

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (наименование.) (должность, Ф.И.О.)

действующим на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (устава, доверенности)

далее - Сторона 2, с другой стороны, совместно именуемые "Стороны", заключили настоящее Соглашение о нижеследующем:

Принятые сокращения и определения

Электронный документооборот - система работы с электронными документами, при которой все электронные документы создаются, передаются и хранятся с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сетевую структуру.

Электронный документ (далее также - ЭД) - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

УЦ - удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи".

ЭП – электронная подпись - 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). Существует простая и усиленная электронная подпись.

Усиленная квалифицированная электронная подпись - вид усиленной ЭП, которая:

-получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

-позволяет определить лицо, подписавшее ЭД;

-позволяет обнаружить факт внесения изменений в ЭД после момента его подписания;

 - создается с использованием средств ЭП.

- ключ проверки электронной подписи указан в квалифицированном сертификате;

- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи".

СКЗИ - средства криптографической защиты информации.

Подписанный электронный документ (далее также - ПЭД) - электронный документ с присоединенной электронной подписью, которая была создана на основе ключа электронной подписи.

Сертификат ключа проверки электронной подписи (далее также - сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. Также называется сертификатом открытого ключа. Сертификат содержит уникальный номер, дату начала и окончания срока действия, сведения о владельце, используемых криптографических алгоритмах, ограничениях на использование, уникальный ключ проверки ЭП, наименование УЦ, выдавшего сертификат, и другую информацию. Сертификат имеет свою ЭП, созданную удостоверяющим центром.

Владелец сертификата ключа проверки электронной подписи (далее также - владелец сертификата) - лицо, которому выдан сертификат ключа проверки электронной подписи. Данные о владельце должны содержаться в сертификате.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания ЭП. Также называется закрытым ключом.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности ЭП (далее - проверка ЭП). Также называется открытым ключом. Значение ключа проверки электронной подписи содержится в сертификате.

Средства электронной подписи (далее также - средства ЭП) - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Корневой сертификат УЦ - сертификат, который был выдан удостоверяющим центром самому себе и является самоподписанным. Все остальные сертификаты, выдаваемые данным УЦ, подписываются ключом ЭП этого корневого сертификата. В понятии инфраструктуры открытых ключей: если есть доверие к корневому сертификату УЦ, то автоматически есть доверие ко всем сертификатам, выданным данным УЦ и подписанным ключом ЭП данного корневого сертификата. Обычно в УЦ есть только один корневой сертификат.

Промежуточный сертификат УЦ - сертификат, ключ ЭП которого использовался для подписи другого сертификата, а сам сертификат был подписан ключом ЭП корневого сертификата УЦ или другого промежуточного сертификата этого УЦ. Промежуточные сертификаты позволяют строить широкую иерархическую структуру сертификатов УЦ.

Самоподписанный сертификат - сертификат, который подписан ключом ЭП, соответствующим ключу проверки ЭП из этого сертификата. В полях издателя сертификата содержатся те же данные, что и в полях владельца сертификата.

Создание ЭП - результат работы средства ЭП при создании ЭП, в результате которого получается последовательность бит данных фиксированной длины после криптографического преобразования электронного документа в хеш и шифрования хеша ключом электронной подписи. Длина названия алгоритмов хеширования и шифрования задаются в сертификате.

Подтверждение подлинности ЭП в ПЭД - положительный результат работы средства ЭП при проверке ЭП. Результат работы считается положительным, если после расшифровывания ЭП с помощью ключа проверки ЭП по заданному в сертификате криптографическому алгоритму получается значение, равное хешу электронного документа, полученному по заданному в Сертификате соответствующему криптографическому алгоритму.

Хеш - результат работы хеширующей функции, которая преобразовывает входной массив данных произвольной длины в выходную битовую строку фиксированной длины.

Участники электронного документооборота - лица, осуществляющие обмен информацией в электронной форме в рамках данного Соглашения.

Компрометация ключа ЭП - нарушение конфиденциальности ключа ЭП, при котором значение закрытого ключа стало известно лицу, не являющемуся владельцем сертификата.

Система - комплекс программно-аппаратных средств, позволяющий осуществлять электронный документооборот между Сторонами в рамках настоящего Соглашения. Система включает в себя средства ЭП и обеспечивает подготовку ЭД, прием, передачу и обработку ПЭД с использованием средств вычислительной техники каждой из Сторон. Передача данных происходит по интернету в Системе автоматизации процессов административно-хозяйственной деятельности центрального аппарата Министерства здравоохранения Российской Федерации (https://web20.ahd-centre.minzdrav.gov.ru).

1. Предмет Соглашения

1.1. Настоящим Соглашением Стороны регламентировали порядок организации между Сторонами защищенного электронного документооборота в целях осуществления документооборота в электронной форме с использованием СКЗИ программного комплекса КриптоПро с функциями шифрования и ЭП.

1.2. Стороны признают электронные документы, заверенные ЭП, при соблюдении требований Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" юридически эквивалентным документам на бумажных носителях, заверенным соответствующими подписями и оттиском печатей Сторон.

1.3. При реализации настоящего Соглашения Стороны обеспечивают конфиденциальность и безопасность персональных данных в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

1.4. Стороны признают, что использование СКЗИ, которые реализуют шифрование и ЭП, достаточно для обеспечения конфиденциальности информационного взаимодействия Сторон, защиты от несанкционированного доступа и безопасности обработки информации, а также для подтверждения того, что:

- электронный документ исходит от Стороны, его передавшей (подтверждение авторства документа);

- электронный документ не претерпел изменений при информационном взаимодействии Сторон (подтверждение целостности и подлинности документа) при положительном результате проверки ЭП;

1.5. Настоящее Соглашение является безвозмездным.

2. Технические условия

2.1. Приобретение, установка и функционирование программного обеспечения, каналов связи, СКЗИ с функциями ЭП осуществляется за счет Сторон, а также с использованием их технических возможностей.

 2.2. Изготовление и сертификацию ключей шифрования и ЭП осуществляют аккредитованные УЦ каждой из Сторон (или– УЦ Федерального казначейства).

2.3. Электронные документы, которые передаются по настоящему Соглашению, должны быть подписаны квалифицированной электронной подписью. Далее в качестве ЭП подразумевается квалифицированная ЭП.

Электронный документ, подписанный квалифицированной электронной подписью, признается документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

2.4. Виды электронных документов, передаваемых другой Стороне:

- акт приема-передачи имущества, приобретенного по централизованным закупкам за счет средств федерального бюджета;

- извещение (форма по ОКУД 0504805);

- акт сверки взаимных расчетов.

2.5. Обмен иными ЭД в Системе не является основанием возникновения обязательств Сторон по Соглашению.

2.6. ПЭД порождает обязательства Сторон, установленные Соглашением, если передающей стороной он должным образом оформлен, подписан ЭП, а принимающей стороной получен, проверен и принят к обработке в установленном Соглашением порядке.

2.7. Данное соглашение распространяется только на обеспечение защиты информации в ПЭД при передаче по открытым каналам связи. Остальные требования по защите информации выполняются Сторонами самостоятельно на основании требований действующего законодательства и требований внутренних нормативных документов Сторон.

2.8. Передача ПЭД осуществляется между Сторонами через Систему.

2.9. Подключение Сторон к интернету выполняется самостоятельно и не является предметом Соглашения.

2.10. Подключение Сторон к Системе осуществляется администратором Системы.

3. Общие принципы электронного документооборота

3.1. Каждая из Сторон при подписании ЭД применяет свой ключ ЭП.

3.2. Перед началом работы Стороны проверяют свои средства ЭП и их подлинность.

3.3. Стороны признают, что:

- внесение изменений в ПЭД дает отрицательный результат проверки ЭП;

- подделка ЭП невозможна без использования ключа ЭП владельца;

- каждая сторона несет ответственность за сохранность своего ключа ЭП и за действия своего персонала при использовании средств ЭП;

- моментом наступления юридической значимости ПЭД является момент получения этого ПЭД через Систему принимающей стороной.

3.4. Стороны признают средства ЭП достаточными для подписания ЭД и проверки подлинности ЭП в ПЭД.

4. Обязанности Сторон

4.1. Стороны обязуются:

4.1.1. Самостоятельно укомплектовать рабочее место владельца сертификата ключа необходимыми программно-техническими средствами и общесистемным программным обеспечением.

4.1.2. Немедленно информировать администратора Системы обо всех случаях утраты, хищения, несанкционированного использования ключей ЭП. При этом работа в Системе приостанавливается до проведения внеплановой смены ключей.

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

4.1.4. Принимать на себя все риски, связанные с работоспособностью своего оборудования и каналов связи.

4.1.5. За собственный счет поддерживать в рабочем состоянии программно-технические комплексы обеспечения работоспособности вычислительной техники и техники связи, обеспечивающих электронный документооборот.

4.1.6. Своевременно (не менее чем за три дня) уведомлять друг друга об изменении своего фактического места нахождения, сетевого адреса в интернете, а также об изменении иных реквизитов, имеющих существенное значение для определения юридического статуса и идентификации Сторон и исполнения обязательств по Соглашению.

4.1.7. Не предпринимать действий, способных нанести ущерб другой стороне вследствие использования Системы.

4.1.8. Своевременно информировать (по электронной почте и/или телефону) другую сторону обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих электронному документообороту.

4.1.9. В случае обнаружения возможных угроз безопасности Стороны обязуются своевременно извещать друг друга о таких угрозах для принятия согласованных мер по их нейтрализации.

4.1.10. Сторона 1, в течение 5 рабочих дней со дня издания распорядительного акта о передаче имущества, направляет Стороне 2 извещение о поставке лекарственных препаратов и акт приема-передачи, приобретенного по централизованным закупкам за счет средств федерального бюджета, подписанные руководителем (уполномоченным лицом) и главным бухгалтером (уполномоченным лицом), а акт сверки взаимных расчетов по мере необходимости.

4.1.11. В случае изменения состава уполномоченных лиц, Стороны обязаны информировать администратора Системы с приложением подтверждающих документов в течение двух рабочих дней с момента принятия таких изменений.

4.1.12. Стороны организуют архивное хранение ПЭД в течение срока действия аналогичных документов, оформленных на бумажных носителях.

5. Права Сторон

5.1. Стороны имеют право:

5.1.1. Ограничивать и приостанавливать использование Системы в случаях ненадлежащего исполнения другой стороной Соглашения с уведомлением не позднее дня приостановления, а по требованию компетентных государственных органов - в случаях и в порядке, предусмотренных законодательством Российской Федерации.

5.1.2. Производить плановую замену ключа ЭП, ключа проверки ЭП и сертификата ключа проверки ЭП по своей инициативе с уведомлением администратора Системы не менее чем за два рабочих дня.

6. Ответственность Сторон и риски убытков

6.1. Стороны несут ответственность за содержание любого ПЭД при условии подтверждения подлинности ЭП.

6.2. Стороны несут ответственность за конфиденциальность и порядок использования ключей ЭП.

6.3. Сторона, допустившая компрометацию ключа ЭП, несет ответственность за ЭД, подписанные с использованием скомпрометированного ключа ЭП, до момента официального уведомления об аннулировании (отзыве) соответствующего сертификата и конкретных документов, подписанных указанным ключом.

6.4. Сторона, несвоевременно сообщившая о случаях утраты или компрометации ключа ЭП, несет связанные с этим риски.

6.5. Если в результате надлежащего исполнения ЭД возникает ущерб для третьих лиц, ответственность несет Сторона, от имени которой ЭД подписан ЭП.

6.6. В случае прекращения действия Соглашения по любому основанию Стороны несут ответственность по обязательствам, возникшим до прекращения действия Соглашения, в соответствии с законодательством Российской Федерации.

7. Порядок смены ключей шифрования и ЭП

7.1. Порядок выдачи, замены ключей шифрования и ЭП, сертификатов ключей подписи, в том числе в случаях их компрометации, для Сторон определяется в соответствии с действующими регламентами УЦ взаимодействующих Сторон.

8. Срок действия Соглашения

8.1. Во всем, что не предусмотрено Соглашением, Стороны руководствуются законодательством Российской Федерации.

8.2. Все споры и разногласия в связи с исполнением Соглашения разрешаются путем

переговоров. Если по результатам переговоров Стороны не приходят к соглашению, спор может быть передан на рассмотрение Арбитражного суда города Москвы.

8.3. Настоящее Соглашение считается заключенным между Участниками электронного документооборота, если оно подписано каждой из Сторон

8.4. Настоящее Соглашение вступает в силу с момента подписания и действует без ограничения срока.

8.5. Стороны могут в одностороннем порядке расторгнуть настоящее Соглашение, письменно уведомив другую Сторону за один месяц.

9. Адреса и реквизиты Сторон

|  |  |
| --- | --- |
| **Сторона 1:**федеральное казенное учреждение«Федеральный центр планированияи организации лекарственногообеспечения граждан» Министерства здравоохранения Российской Федерации(ФКУ «ФЦПиЛО» Минздрава России)Юридический адрес: 109044, г.Москва, ул. Воронцовская, д.6, стр1.Тел. +7(495)249 03 01e-mail: fcpilo.info@minzdrav.gov.ru | **Сторона 2:**Наименование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Юридический адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Тел./факс \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_e-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 Подписи Сторон

 Сторона 1: Сторона 2:

 \_\_\_\_\_\_\_\_\_\_/ Е.А. Максимкина \_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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