ПРАВИТЕЛЬСТВО СВЕРДЛОВСКОЙ ОБЛАСТИ

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ СВЕРДЛОВСКОЙ ОБЛАСТИ
МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ

ПРИКАЗ

30 августа 2023 № 306/2012-П

г. Екатеринбург

Об утверждении регламента по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с единой государственной информационной системой в сфере здравоохранения Свердловской области

Во исполнение постановления Правительства Российской Федерации от 01.06.2021 № 852 «О лицензировании медицинской деятельности», постановления Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения», приказа Министерства здравоохранения Российской Федерации от 07.09.2020 № 947н «Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов», а также Национальных стандартов серии «Информатизация здоровья»

ПРИКАЗЫВАЕМ:

1. Министерству цифрового развития и связи Свердловской области обеспечить на территории Свердловской области возможность подключения медицинских учреждений Свердловской области частной формы собственности (далее — МО ЧСЗ) к Единой государственной информационной системе в сфере здравоохранения Свердловской области (далее — ЕГИСЗ СО) с целью обеспечения взаимодействия МО ЧСЗ с Единой государственной информационной системой здравоохранения (далее — ЕГИСЗ) с использованием собственной медицинской информационной системы (далее — МИС) МО ЧСЗ, а также предусмотреть возможность подключения к МИС Свердловской области (далее — МИС СО), в случае отсутствия собственной МИС ЧСЗ, для доступа к ЕГИСЗ.

2. Утвердить регламент по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с единой государственной информационной системой в сфере здравоохранения Свердловской области, включающий порядок подключения МИС МО ЧСЗ (далее — регламент) (прилагается).

3. Руководителям МО ЧСЗ и участникам информационного взаимодействия при подключении к ЕГИСЗ СО руководствоваться регламентом, утвержденным настоящим приказом, а также следовать порядку подключения МО ЧСЗ к ЕГИСЗ СО, доступному на официальном сайте оператора технической поддержки в информационно–телекоммуникационной сети «Интернет» (https://egov66.ru/mis/).

4. Руководителю медицинского информационно–аналитического центра ГАУДПО «Уральский институт управления здравоохранением имени А.Б. Блохина» М.В. Фомину:

1) организовать информирование МО ЧСЗ о необходимости и возможностях подключения к ЕГИСЗ СО;

2) оказать содействие в подключении МО ЧСЗ к Федеральному реестру медицинских организаций и Федеральному регистру медицинских работников (далее – ФРМР/ФРМО), обеспечить консультационно–методическую помощь МО ЧСЗ в части подключения и внесения данных в ФРМР/ФРМО МО ЧСЗ.

5. Директору ГБУ СО «Оператор электронного правительства» Е.А. Гуляевой организовать подключение МО ЧСЗ к ЕГИСЗ посредством МИС СО в соответствии с регламентом при выполнении мероприятий, предусмотренных порядком подключения.

6. Контроль за исполнением настоящего приказа оставляем за собой.

Министр цифрового развития и связи Свердловской области	Министр здравоохранения Свердловской области
_____ М.Я. Пономарьков	_____ А.А. Карлов

УТВЕРЖДЕН
приказом Министерства цифрового развития и связи Свердловской области и Министерства здравоохранения Свердловской области
от 30.08.2023 № 306/2012-П
«Об утверждении Регламента по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с медицинскими информационными системами Свердловской области для обеспечения доступа к единой государственной информационной системы в сфере здравоохранения»

Регламент
по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с единой государственной информационной системой в сфере здравоохранения Свердловской области

Глава 1. Общие положения

1.1. Настоящий регламент по организации информационного взаимодействия медицинских информационных систем (далее – МИС) медицинских организаций частной системы здравоохранения (далее – МО ЧСЗ) с единой государственной информационной системой в сфере здравоохранения Свердловской области (далее – ЕГИСЗ СО) с целью взаимодействия с Единой государственной информационной системой (далее – ЕГИСЗ) (далее – Регламент) определяет порядок подключения к ЕГИСЗ МИС медицинских организаций (далее – МО) государственной и частной систем здравоохранения и иных информационных систем.

1.2. Ключевым принципом организации информационного взаимодействия является обеспечение возможности обмена данными между информационными системами в сфере здравоохранения о случаях оказания медицинской помощи в электронном виде в объеме, необходимом и достаточном для обеспечения преемственности и непрерывности процессов оказания медицинской помощи в отношении отдельно взятого пациента.

Под информационным взаимодействием с подсистемами ЕГИСЗ понимается организация информационного взаимодействия со следующими подсистемами ЕГИСЗ:

– федеральный регистр медицинских работников;

– федеральный реестр медицинских организаций;

– федеральная электронная регистратура;

– федеральная интегрированная электронная медицинская карта;

– федеральный реестр электронных медицинских документов;

– подсистема ведения специализированных регистров пациентов по отдельным нозологиям и категориям граждан, мониторинга организации оказания высокотехнологичной медицинской помощи и санаторно–курортного лечения;

– федеральный реестр нормативно–справочной информации в сфере здравоохранения;

– подсистема автоматизированного сбора информации о показателях системы здравоохранения из различных источников и представления отчетности.

Информационное взаимодействие с указанными подсистемами ЕГИСЗ осуществляется с помощью соответствующих сервисов ЕГИСЗ СО.

Правила взаимодействия информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг (далее – Иных ИС), участвующих в информационном взаимодействии с ЕГИСЗ, информационными системами в сфере здравоохранения и медицинскими организациями утверждены постановлением Правительства Российской Федерации от 12 апреля 2018 г. № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями».

Посредством ЕГИСЗ СО и МИС МО осуществляется информационное взаимодействие МИС МО ЧСЗ со следующими федеральными информационными системами:

– информационные системы участников информационного взаимодействия, указанных в Положении о ЕГИСЗ, утвержденном постановлением Правительства Российской Федерации от 09.02.2022 № 140;

– Личный кабинет пациента «Мое здоровье» на Едином портале государственных услуг и функций;

– Вертикально–интегрированные медицинские информационные системы (далее – ВИМИС) по следующим направлениям организации оказания медицинской помощи:

– организация оказания медицинской помощи больным онкологическими заболеваниями – ВИМИС «Онкология»;

– организация оказания медицинской помощи больным сердечно–сосудистыми заболеваниями – ВИМИС «ССЗ»;

– организация оказания медицинской помощи по профилям «Акушерство и гинекология» и «Неонатология» (Мониторинг беременных) – ВИМИС «АКиНЕО»;

– организация оказания профилактической медицинской помощи (диспансеризация, диспансерное наблюдение, профилактические осмотры) – ИМИС «Профилактическая медицина».

Информационное взаимодействие МИС МО ЧСЗ с ЕГИСЗ осуществляется с использованием защищенной сети передачи данных (далее – ЗСПД).

1.3. Регламент распространяется на информационный обмен участников системы информационного взаимодействия при направлении электронных медицинских документов в ЕГИСЗ.

1.4. Участниками информационного взаимодействия в ЕГИСЗ СО являются Министерство здравоохранения Свердловской области, медицинские организации Свердловской области, иные учреждения, организации, заключившие договор с государственным бюджетным учреждением Свердловской области «Оператор электронного правительства» (далее – ГБУ СО «Оператор электронного правительства») в части подключения и предоставления доступа к ЕГИСЗ СО, являющиеся поставщиками и/или потребителями сведений компонентов ЕГИСЗ СО, физические лица: пользователи ЕГИСЗ СО, являющиеся сотрудниками участников информационного взаимодействия в ЕГИСЗ СО, и пациенты.

1.4. Оператором ЕГИСЗ СО является ГБУ СО «Оператор электронного правительства» либо определяемое им юридическое лицо на основании заключенного договора об оказании услуг по выполнению функций оператора на территории Свердловской области (далее – оператор ЕГИСЗ СО).

1.5. Поставщиками информации являются государственные учреждения здравоохранения Свердловской области, МО ЧСЗ, индивидуальные предприниматели, осуществляющие медицинскую деятельность на территории Свердловской области (далее – поставщики информации).

1.6. Пользователями являются должностные лица (специалисты, сотрудники) учреждений здравоохранения Свердловской области, органов управления сферой здравоохранения Свердловской области, аптечных организаций, имеющих доступ к ограниченному функционалу ЕГИСЗ СО (далее – пользователи ЕГИСЗ СО).

1.7. Участниками системы информационного взаимодействия являются:

1) оператор ЕГИСЗ СО;

2) поставщики информации;

3) пользователи ЕГИСЗ СО.

1.8. Информационные системы участников системы информационного взаимодействия должны соответствовать требованиям законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

1.9. Оператор и поставщики информации при обработке персональных данных принимают необходимые правовые, организационные и технические меры для защиты персональных данных и сведений, отнесенных к врачебной тайне, от неправомерного или случайного доступа к ним, уничтожения, изменения,

блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

Глава 2. Порядок подключения к МИС МО

2.1. Подключение к ЕГИСЗ СО производится при выполнении требований по обеспечению безопасности персональных данных, предусмотренных законодательством Российской Федерации, нормативными правовыми актами Свердловской области и настоящим положением. Руководители МО ЧСЗ, заключившие договор об использовании ЕГИСЗ СО, являются ответственными за допуск своих сотрудников к МИС МО ЧСЗ, ЕГИСЗ СО.

2.2. МО ЧСЗ обеспечивают за счет собственных средств подключение к ведомственной защищенной сети передачи данных здравоохранения Свердловской области (ViPNet–сеть № 1691), в которой обеспечивается защита обрабатываемой информации, в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, на основании Федерального закона от 27 июля 2006 года № 149–ФЗ «Об информации, информационных технологиях и о защите информации», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, Федеральным законом от 27 июля 2006 года № 152–ФЗ «О персональных данных», постановлением Правительства Российской от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации», приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и требованиями раздела II приказа Минздрава России от 24 декабря 2018 года № 911н.

2.3. МО ЧСЗ необходимо зарегистрироваться в Федеральном реестре медицинских организаций (далее – ФРМО). Медицинским работникам необходимо зарегистрироваться в Федеральном реестре медицинских работников (далее – ФРМР) и внести информацию о медицинских работниках МО ЧСЗ.

Регистрация осуществляется МО ЧСЗ в порядке, установленном Положением о единой государственной информационной системе в сфере здравоохранения, утвержденным постановлением Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения» (ссылка на регистрацию: https://frmo.minzdrav.gov.ru/reg–frmo).

2.4. МО ЧСЗ необходимо направить официальный запрос в адрес Министерства здравоохранения Свердловской области на подключение к ЕГИСЗ

СО и ведомственной защищенной сети передачи данных здравоохранения Свердловской области (ViPNet–сети № 1691) с указанием обоснования подключения, необходимого функционала в МИС МО и подтверждением выполнения требований по защите информации (аттестат соответствия требованиям по защите информации, выданный на основании аттестационных мероприятий, проведенных организацией, лицензиатом ФСТЭК России).

2.5. Средства защиты информации для обеспечения информационной безопасности автоматизированных рабочих мест, в том числе средства криптографической защиты информации ведомственной защищенной сети передачи данных здравоохранения Свердловской области (ViPNet–сети № 1691), приобретаются МО ЧСЗ самостоятельно.

2.6. Министерство здравоохранения Свердловской области согласовывает подключение МО ЧСЗ к ЕГИСЗ СО и информирует об этом МО ЧСЗ, а также направляет в адрес Министерства цифрового развития и связи Свердловской области официальное письмо о согласии на подключение МО ЧСЗ к ЕГИСЗ СО с подтверждением выполнения необходимых требований и функционала.

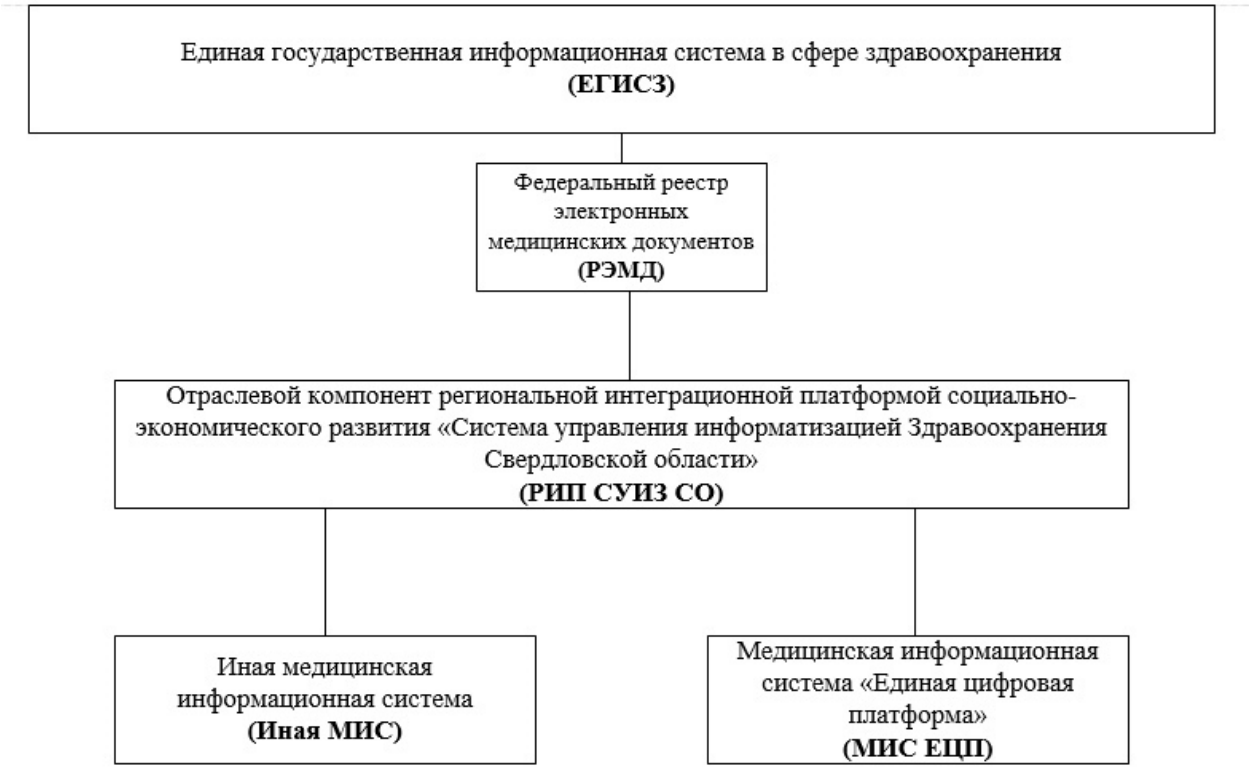
После получения официального ответа от Министерства здравоохранения Свердловской области о согласовании подключения к ЕГИСЗ СО МО ЧСЗ направляет в адрес оператора ЕГИСЗ СО в службу технической поддержки на адрес электронной почты sd@egov66.ru ответ о согласовании подключения Министерства здравоохранения Свердловской области, а также согласованные заявки (приложение № 1, приложение № 2).

2.7. Подключение осуществляется на основании действующих технических требований оператора ЕГИСЗ СО, публикуемых в открытом доступе в сети «Интернет» (https://egov66.ru). Подключение и использование МО ЧСЗ ведомственной защищенной сети передачи данных здравоохранения Свердловской области (ViPNet–сети № 1691) и МИС осуществляется за счет собственных средств МО ЧСЗ.

2.8. Подключаясь к ЕГИСЗ СО, поставщики информации несут ответственность за полноту, достоверность и своевременную актуализацию данных.

2.9. МО ЧСЗ, являющиеся участниками информационного взаимодействия, доводят до потребителей информацию о возможности использования электронных медицинских документов через свои территориально обособленные структурные подразделения на своих ресурсах в информационно–телекоммуникационной сети «Интернет», а также иными разрешенными законодательством способами.

Схема взаимодействия с подсистемой «Реестр электронных медицинских документов» ЕГИСЗ посредством использования МИС «Единая цифровая платформа» или иной МИС, использующейся с МО ЧСЗ



Взаимодействие с ЕГИСЗ основано на передаче СЭМД, которые формируются и подписываются в МИС.

Глава 3. Требования к организации информационного взаимодействия

Министерство цифрового развития и связи Свердловской области, как орган исполнительной власти субъекта Российской Федерации, уполномоченный высшим исполнительным органом государственной власти субъекта Российской Федерации на создание, развитие и эксплуатацию ЕГИСЗ СО совместно с Министерством здравоохранения Свердловской области, а также оператор ЕГИСЗ СО, разрабатывает и публикует требования и регламент организации взаимодействия МИС МО ЧСЗ с ЕГИСЗ СО в целях включения МО ЧСЗ в единый цифровой контур здравоохранения.

Указанные документы основываются на модели, принятой в Свердловской области для МО государственной и муниципальной системы здравоохранения, с учетом технических и архитектурных особенностей, а также финансово–экономической модели ЕГИСЗ СО, и должны содержать информацию о технических аспектах подключения в виде инструкций, методических рекомендаций, интеграционных профилей. Указанные документы в обязательном порядке должны содержать описание механизма проверки документов, подтверждающих соответствие МИС МО ЧСЗ и иных информационных систем

требованиям безопасности информации, определенным законодательством и нормативными правовыми актами Российской Федерации в области защиты информации.

Министерство цифрового развития и связи Свердловской области разрабатывает и поддерживает в актуальном состоянии типовой договор с МО ЧСЗ в части подключения и предоставления доступа к ЕГИСЗ СО. Типовой договор должен содержать положения о времени, месте, сроках, этапности, условиях подключения и предоставления доступа к ЕГИСЗ СО, правах и обязанностях, ответственности сторон (включая организацию технической поддержки).

В случае, если МО ЧСЗ участвует в территориальной Программе государственных гарантий бесплатного оказания гражданам медицинской помощи в субъекте Российской Федерации, в регламенте по организации взаимодействия МИС МО ЧСЗ с ЕГИСЗ СО должны быть учтены следующие положения:

– в целях мониторинга доступности записи на прием к врачу в сроки, установленные программой государственных гарантий бесплатного оказания гражданам медицинской помощи, оператор ЕГИСЗ СО обеспечивает доступ МИС МО ЧСЗ к системе (подсистеме) «Управление потоками пациентов» (электронной регистратуре) ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему);

– МО ЧСЗ обеспечивает своевременную передачу информации в ЕГИСЗ в целях проведения сравнительного анализа деятельности медицинских организаций, а также анализа обеспеченности и потребности в основных видах медицинской помощи, включая контроль выполнения территориальной программы государственных гарантий бесплатного оказания гражданам медицинской помощи;

– МО ЧСЗ, имеющая прикрепленное население в рамках Программы государственных гарантий бесплатного оказания гражданам медицинской помощи, должна обеспечивать учет прикрепленного к МО ЧСЗ и медицинскому работнику населения, своевременное направление информации о прикреплении пациентов в информационные системы территориального фонда обязательного медицинского страхования, страховых медицинских организаций и ЕГИСЗ СО;

– в целях осуществления сбора, систематизации и обработки сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования, обмена структурированными электронными медицинскими документами между МИС МО, ЕГИСЗ СО и подсистемой «Федеральная интегрированная электронная медицинская карта» ЕГИСЗ оператор ЕГИСЗ СО предоставляет возможность подключения МИС МО ЧСЗ к централизованной системе (подсистеме) «Ведение интегрированных электронных медицинских карт пациентов» ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему);

– в целях обеспечения обращения рецептов на лекарственные препараты, сформированных в форме электронных документов, организации учета информации о лекарственном препарате и его обслуживании аптечными организациями, учета выданных рецептов с проверкой льготы пациента путем получения соответствующих первичных сведений из медицинских

информационных систем, передачи данных о выданных рецептах в ЕГИСЗ СО, Министерство цифрового развития и связи Свердловской области совместно с оператором ЕГИСЗ СО предоставляет возможность подключения МИС МО ЧСЗ к централизованной системе (подсистеме) «Управление льготным лекарственным обеспечением» ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему);

– МО ЧСЗ осуществляет доработку МИС в целях подключения ко всем федеральным сервисам в случае использования собственной МИС.

При необходимости МО ЧСЗ могут учитываться следующие положения:

– в целях осуществления сбора, централизованного хранения и обеспечения оперативного доступа к имеющимся данным лабораторных исследований с автоматизированных рабочих мест медицинских работников при осуществлении ими своей профессиональной деятельности в рамках субъекта Российской Федерации, проводящих лабораторную диагностику и лечебно–диагностический процесс, а также обеспечения возможности анализа обоснованности назначений лабораторных исследований (в том числе повторных) Министерство цифрового развития и связи Свердловской области, организация, назначенная указанным органом, предоставляет возможность подключения МИС МО ЧСЗ к централизованной системе (подсистеме) «Лабораторные исследования» ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему);

– в целях осуществления централизованного хранения в электронном виде результатов диагностических исследований (медицинских изображений, формируемых в МО ЧСЗ, выполняющих диагностические исследования), предоставления оперативного доступа к имеющимся результатам диагностических исследований (медицинских изображений) с автоматизированных рабочих мест медицинских работников при осуществлении ими профессиональной деятельности, а также обеспечения возможности анализа обоснованности назначений диагностических исследований (в том числе повторных) Министерство цифрового развития и связи Свердловской области, организация, назначенная указанным органом, предоставляет возможность подключения МИС МО ЧСЗ к централизованной системе (подсистеме) хранения и обработки результатов диагностических исследований (медицинских изображений) »Центральный архив медицинских изображений» ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему);

– в целях оказания медицинской помощи с применением телемедицинских технологий на территории субъекта Российской Федерации на межрегиональном и федеральном уровне в соответствии с порядком организации и оказания медицинской помощи с применением телемедицинских технологий, утвержденным приказом Министерства здравоохранения Российской Федерации от 30 ноября 2017 г. № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий», Министерство цифрового развития и связи Свердловской области, организация, назначенная указанным органом, предоставляет возможность подключения МИС МО ЧСЗ к централизованной системе (подсистеме) «Телемедицинские

консультации» ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему);

– в целях интеграции с региональными центрами приема и обработки вызовов, контроля времени доезда санитарного автотранспорта, маршрутизации пациентов при неотложных состояниях в специализированные медицинские организации, обеспечения доступа врачу скорой помощи к сведениям об аллергическом статусе и хронических диагнозах пациентов Министерство цифрового развития и связи Свердловской области, организация, назначенная указанным органом, предоставляет возможность подключения МИС МО ЧСЗ к централизованной системе (подсистеме) «Управления скорой и неотложной медицинской помощи (в том числе санитарной авиации)» ЕГИСЗ СО, а МО ЧСЗ обеспечивает своевременное предоставление информации в указанную систему (подсистему).

Министерство цифрового развития и связи Свердловской области, организация, назначенная указанным органом, разрабатывает и поддерживает в актуальном состоянии типовой договор с операторами Иных ИС в части подключения и предоставления доступа к ЕГИСЗ СО. Типовой договор должен содержать положения о времени, месте, сроках, этапности, условиях подключения и предоставления доступа к ЕГИСЗ СО, правах и обязанностях, ответственности сторон (включая организацию Технической поддержки).

Глава 4. Описание требований к медицинским информационным системам МО ЧСЗ

4.1. Общие требования

Для интеграции с МИС МО должны быть выполнены следующие условия:

– ИС должна удовлетворять требованиям к защите информации, установленным действующим законодательством, обеспечивать защиту конфиденциальной информации и персональных данных в соответствии с классификацией информации и объектов информатизации, на которых осуществляется обработка данных категорий информации;

– медицинские организации, участвующие в создании электронных медицинских документов, должны быть зарегистрированы в ФРМО;

– сотрудники МО, участвующие в создании электронных медицинских документов, должны быть внесены в ФРМР (должно быть заполнено в размере необходимых данных).

4.2. Требования к каналу передачи данных

Информационный обмен через интеграционные сервисы в промышленной среде должен производиться с использованием защищенных сетей передачи данных, построенных на базе продуктов ViPNet (эквивалент не допускается в целях обеспечения совместимости с уже имеющимся программным обеспечением). Организация защищенного информационного обмена происходит с помощью защищенных сетей передачи данных здравоохранения Свердловской области (ViPNet–сеть № 1691).

Пропускная способность канала связи, используемого для информационного обмена, должна составлять не менее 10 Мбит/с.

4.3. Требования нормативно–правовых актов в сфере защиты информации.

Согласно Приказу ФСТЭК России от 11.02.2013 № 17 на автоматизированных рабочих местах должны быть реализованы следующие меры защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных

Для организации подключения к МИС МО с целью передачи данных в ФРЭМД ЕГИСЗ на автоматизированных рабочих местах необходимо установить и настроить сертифицированные средства защиты информации и провести приемочные испытания системы защиты информации объекта информатизации.

Сертифицированные средства защиты информации, требуемые к установке:

- СЗИ от НСД (Secret Net или Dallas Lock);
- Kaspersky Endpoint Security для бизнеса – Стандартный;
- Программное обеспечение ViPNet Client (в пределах контролируемой зоны может быть размещен ViPNet Coordinator, если требуется подключение нескольких автоматизированных рабочих мест. Применяемые криптографические средства защиты информации должны быть полностью совместимы с уже существующими средствами защиты каналов связи – ведомственной защищенной сетью передачи данных здравоохранения Свердловской области (ViPNet–сетью № 1691).

Подтверждение выполнения вышеуказанных мероприятий осуществляется посредством прикрепления к письму следующих сканированных документов:

1. Аттестат соответствия требованиям по защите информации, выданный на основании аттестационных мероприятий, проведенных организацией лицензиатом ФСТЭК России.
2. Акт приемо–сдаточных испытаний объекта информатизации.
3. Приказ о назначении администратора информационной безопасности.
4. Приказ о назначении ответственных за обработку ПДН.
5. Лицензия на осуществление медицинской деятельности

Глава 5. Требования по защите информации при подключении медицинских организаций частной системы здравоохранения к медицинским информационным системам Свердловской области и обеспечения доступа к единой государственной информационной системы в сфере здравоохранения

Технические и организационные меры по защите информации в единой государственной информационной системе в сфере здравоохранения Свердловской области (далее – ЕГИСЗ) разработаны на основании следующих руководящих документов:

– Федерального закона от 27 июля 2006 года № 149–ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27 июля 2006 года № 152–ФЗ «О персональных данных»;

– постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановления Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения»;

– приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

– приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказа Министерства здравоохранения Российской Федерации от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

Глава 6. Мероприятия по защите информации при подключении к ЕГИСЗ.

6.1. Общие требования

При подключении к медицинским информационнымсистемам должны быть реализованы следующие меры защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

Подтверждение реализации указанных мер защиты информации осуществляется посредством предоставления сканированных копий документов:

- аттестат соответствия требованиям по защите информации, выданный на основании аттестационных мероприятий, проведенных организацией лицензиатом ФСТЭК России;
- акт приемо–сдаточных испытаний объекта информатизации;
- приказ о назначении администратора информационной безопасности;
- приказ о назначении ответственных за обработку ПДН.

6.2.Организационные мероприятия по обеспечению безопасности информации.

Комплекс организационных мероприятий по защите информации при подключении к единой государственной информационной системы в сфере здравоохранения Свердловской области, должен включать в себя следующие меры:

- все технические средства обработки информации и носители информации должны быть размещены в пределах контролируемой зоны;
- все помещения, в которых происходит обработка и хранение защищаемой информации, а также помещение с оборудованием, обеспечивающим технологический процесс обработки информации, должны быть оснащены средствами охранно–пожарной сигнализации;
- входные двери в помещения должны быть оснащены надежными замками;
- допуск в помещения вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) должен производиться только

в случае служебной необходимости в присутствии лиц, ответственных за эксплуатацию помещений;

– физическая охрана технических средств информационной системы должна предусматривать контроль доступа в помещения;

– должно проводиться резервирование технических средств, дублирование массивов и носителей информации;

– должен быть определен перечень лиц, допущенных к обработке информации в ИС;

– должен быть назначен ответственный за обеспечение безопасности информации;

– все машинные носители информации, средства защиты информации должны быть учтены в специальных журналах.

Глава 7.Технические мероприятия по обеспечению безопасности информации

7.1 Общие требования к реализации технических мероприятий по обеспечению безопасности информации.

Применяемые технические средства защиты информации должны соответствовать требованиям к средствам защиты информации, определенным в пункта 26 Приказа ФСТЭК России от 11.02.2013 г. № 17 для информационных систем 2 класса защищенности.

Выбранные для использования сертифицированные по требованиям безопасности информации средства защиты должны соответствовать:

– средства вычислительной техники – не ниже 5 класса в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– системы обнаружения вторжений и средства антивирусной защиты – не ниже 4 класса защиты;

– межсетевые экраны – не ниже 3 класса в соответствии с РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– программное обеспечение СЗИ – не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей в соответствии с РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

7.2 Обеспечение безопасности информации при передаче по телекоммуникационным каналам связи.

При передаче информации по телекоммуникационным каналам связи необходимо обеспечить защиту передаваемой информации от несанкционированного доступа к ней криптографическими средствами защиты информации.

Применяемые криптографические средства защиты информации должны быть полностью совместимы с уже существующими средствами защиты каналов связи (ViPNet–сеть № 1691, в составе: ПО ViPNet Administrator, ПАК ViPNet Coordinator HW1000, ПАК ViPNet Coordinator HW100C).

Класс применяемых криптографических средств зависит от мер, реализованных в учреждении по обеспечению безопасности информации и определяется в соответствии со следующими рекомендациями:

– в случае реализации комплекса мероприятий организационного и технического характера, обеспечивающего отсутствие несанкционированного доступа к автоматизированным рабочим местам (далее – АРМ) пользователей медицинских информационных систем со стороны потенциально возможных внутренних нарушителей безопасности информации (сотрудников и внешних посетителей, не являющихся зарегистрированными пользователями, имеющими право постоянного или разового доступа в контролируемую зону в которой расположен АРМ Пользователя), достаточными средствами криптографической защиты информации являются средства класса КС1;

– в случае отсутствия комплекса мероприятий организационного и технического характера, обеспечивающего отсутствие несанкционированного доступа к АРМ Пользователей медицинских информационных систем со стороны потенциально возможных внутренних нарушителей безопасности информации необходимо применять средства криптографической защиты информации класса не ниже КС2.

7.3. Порядок проведения мероприятий по защите информации в информационных системах при подключении к медицинским информационным системам Свердловской области.

Для проведения работ по защите информации при подключении к медицинским информационным системам необходимо руководствоваться нормативными документами, перечисленными в разделе № 1 текущего документа, для проведения указанных мероприятий допускается привлечение организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04 мая 2011 года № 99–ФЗ «О лицензировании отдельных видов деятельности».

7.4. Рекомендации к средствам защиты информации.

Применяемые технические средства защиты информации должны быть сертифицированы ФСТЭК России (ФСБ России в части средств криптографической защиты информации) и соответствовать требованиям к средствам защиты информации определенным:

– приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для информационных систем 2 класса защищенности;

– приказом ФСТЭК от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– приказом ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»;

– приказом ФСТЭК России от 20 марта 2012 г. № 28 «Требования к средствам антивирусной защиты»;

– иных нормативных, руководящих документов и методических рекомендаций в области обеспечения безопасности информации.

Меры по защите АРМ пользователей медицинских информационных систем определяются самостоятельно (или с привлечением организаций – лицензиатов ФСТЭК России и ФСБ России по направлениям технической и криптографической защиты информации) в зависимости от уже реализованных в учреждении мер организационного и технического характера по обеспечению безопасности информации в соответствии с требованиями федеральных законов и нормативных документов ФСТЭК России и ФСБ России, а также в соответствии с требованиями настоящего документа.

При выборе средств защиты необходимо руководствоваться следующими рекомендациями:

№ п/п	**Средства защиты информации**	
1	Средства антивирусной защиты	Средства антивирусной защиты должны быть лицензионными и сертифицированными ФСТЭК России с ежедневно обновляемыми базами сигнатур. (Kaspersky Endpoint Security – медиапак)
2	Средства защиты информации при передаче по каналам связи	Применяемые средства должны быть полностью совместимы с уже существующими средствами защиты каналов связи (ViPNet–сеть № 1691) (ViPNet Coordinator HW, ViPNet Client, или аналоги)
3	Средства межсетевого экранирования	Средства межсетевого экранирования должны корректно функционировать в рамках существующей ЗСПД (ViPNet Coordinator HW, ViPNet Client, или аналоги)
4	Системы обнаружения вторжений	Системы обнаружения вторжений должны корректно функционировать в рамках существующей системы защиты информации. В качестве средства обнаружения вторжений допустимо использование программно – аппаратного комплекса ViPNet IDS 1000, который корректно функционирует в действующей развернутой сети ViPNet
5	Средства защиты от несанкционированного доступа с программным модулем доверенной загрузки	Средства защиты должны быть способны корректно функционировать на рабочих стациях. **Вариант № 1** Dallas Lock 8.0–С или аналоги с программным модулем доверенной загрузки **Вариант № 2**

6	Средства доверенной загрузки	Средство от НСД SecretNet или аналоги Средства ДЗ ПАК Соболь или аналоги

Глава 8. Подключение к медицинским информационным системам.

Подключение к медицинским информационным системам производится по договору между оператором ЕГИСЗ СО и руководителями учреждений и организаций, планирующих осуществить подключение к информационной системе.

Подключение АРМ пользователей к МИС производится только после выполнения учреждением всех требований по обеспечению информационной безопасности (в том числе в части персональных данных), предусмотренных федеральными законами, нормативными документами и определенными настоящим документом.

Предоставление доступа пользователей к государственным информационным системам должно осуществляется на основании заявок, оформленных установленным порядком, проект заявки прилагается (Приложение № 1).

Ответственными за допуск учреждений и организаций к медицинским информационным системам являются операторы данных систем.

Ответственными за допуск сотрудников к медицинским информационным системам являются руководители учреждений и организаций, подключенных к ЕГИСЗ.

Глава 9. Нормативно–правовая база и стандарты

При организации информационно–телекоммуникационного взаимодействия МИС МО ЧСЗ с МИС МО и подсистемами ЕГИСЗ необходимо руководствоваться следующими нормативными правовыми актами и стандартами:

– Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323–ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Федеральный закон Российской Федерации от 21 июля 2017 г. № 242–ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»;

– Федеральный закон от 27 июля 2006 г. № 152–ФЗ «О персональных данных»;

– Федеральный закон от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 26 июля 2017 г. № 187–ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– постановление Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения»;

– постановление Правительства Российской Федерации от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации,

касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями»;

– постановление Правительства Российской Федерации от 16.12.2017 № 1567 «Об утверждении Правил информационного взаимодействия страховщика, страхователей, медицинских организаций и федеральных государственных учреждений медико–социальной экспертизы по обмену сведениями в целях формирования листка нетрудоспособности в форме электронного документа»;

– постановление Правительства Российской Федерации от 14.12.2018 № 1556 «Об утверждении Положения о системе мониторинга движения лекарственных препаратов для медицинского применения»;

– постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

– постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

– постановление Правительства Российской Федерации от 07.08.2019 № 1026 «О применении пункта 19(1) требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

– постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;

– приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения

и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

– приказ ФСБ России от 24.11.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

– приказ ФОМС от 07.04.2011 № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования»;

– приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

– приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– национальный проект «Здравоохранение», утвержденный 24.12.2018 президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам;

– приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам и информационным системам фармацевтических организаций»;

– приказ Минздрава России от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий»;

– «Основные разделы электронной медицинской карты», утвержденные Минздравом России 11.11.2013 № 18–1/1010;

– ГОСТ Р 52636–2006 «Электронная история болезни. Общие положения»;

– ГОСТ Р 51624–2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

– ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»;

– ГОСТ Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

– ГОСТ Р 53114–2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;

– ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

– национальные стандарты серии «Информатизация здоровья».

Глава 9. Список ссылочных документов

Актуальные версии документов находятся в разделе «Материалы» на портале оперативного взаимодействия участников ЕГИСЗ, доступном по ссылке http://portal.egisz.rosminzdrav.ru/materials.

1. Методические материалы по подключению к Сервису ИПС: http://portal.egisz.rosminzdrav.ru/materials/11;
2. ФРМО. Описание интеграционных профилей: https://portal.egisz.rosminzdrav.ru/materials/481;
3. ФРМР. Описание интеграционных профилей: https://portal.egisz.rosminzdrav.ru/materials/483;
4. Материалы по подсистеме «Федеральный реестр электронных медицинских документов»:

   https://portal.egisz.rosminzdrav.ru/materials/categories/853;
5. Регламент предоставления услуги подключения к защищенной сети передачи данных (ЗСПД) Министерства здравоохранения Российской Федерации региональных медицинских организаций: https://portal.egisz.rosminzdrav.ru/materials/3533.

Приложение № 1
к Регламенту по организации
информационного взаимодействия
медицинских информационных систем
медицинских организаций частной
системы здравоохранения
с медицинскими информационными
системами Свердловской области
для обеспечения доступа к единой
государственной информационной
системы в сфере здравоохранения»

Заявка на подключение к
единой государственной информационной системе в сфере здравоохранения

Прошу предоставить доступ к единой государственной информационной системы в сфере здравоохранения для работы в (подсистема МИС)

Данные об органе/организации			
Полное наименование органа/организации			
Краткое наименование органа/организации			
Данные об уполномоченном должностном лице органа/организации			
№ п/п	Фамилия, Имя отчество	СНИЛС	Рабочий телефон Адрес электронной почты
1			
2			
3			
Данные о проведении мероприятий по защите информации			
Дата и номер аттестата соответствия			
Используемые средства защиты информации			
ФИО, контактная информация администратора безопасности			
Данные о согласовании доступа с оператором медицинских информационных систем			
Номер и дата письма о согласовании доступа			
Кем согласовано (Должность, ФИО)			

Руководитель _____ Фамилия, Инициалы

(дата)

Приложение № 2
к Регламенту по организации
информационного взаимодействия
медицинских информационных систем
медицинских организаций частной
системы здравоохранения
с медицинскими информационными
системами Свердловской области
для обеспечения доступа к единой
государственной информационной
системы в сфере здравоохранения»

Форма заявки на предоставление доступа частной медицинской организации к промышленной среде МИС МО (указать наименование медицинской информационной системы) Свердловской области

Прошу предоставить пользователям право на доступ. Сведения о пользователях приведены в таблице 1.

Таблица 1. Сведения о пользователях

№ п/п	СНИЛС	ФИО (полностью)	Адрес электронной почты	Субъект РФ	Полное наименование организации	Краткое наименование организации	Наименование подсистемы, в которую необходим доступ	Наименование роли
1.				Свердловская область	Министерство здравоохранения Свердловской области	МЗ СО		
2.								

Министр

_____ / Карлов А.А./

М.П.