ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ИВАНОВСКОЙ ОБЛАСТИ

П Р И К А З

от 28.12.2024 № 147

Об утверждении Регламента подключения к государственной информационной системе в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области»

В соответствии с постановлением Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения», руководствуясь подпунктом 4.3.13 пункта 4.3 Положения о Департаменте здравоохранения Ивановской области, утвержденного постановлением Правительства Ивановской области от 28.12.2012 № 578-п, в целях обеспечения информационной безопасности при передаче информации между участниками информационного взаимодействия с единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ) **приказываю:**

1.Утвердить Регламент подключения к государственной информационной системе в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области» в соответствии с приложением к настоящему приказу.

2. Признать утратившими силу:

2.2.1. Приказ Департамента здравоохранения Ивановской области от 09.08.2023 № 219 «Об утверждении регламента подключения к региональной медицинской информационной системе системы здравоохранения Ивановской области (РМИС СЗ ИО) медицинских организаций, не подведомственных Департаменту здравоохранения Ивановской области для информационного взаимодействия с ЕГИСЗ».

2.2.2. Регламент подключения к региональной медицинской информационной системе (РМИС СЗ ИО) Ивановской области, утвержденный 07.04.2022.

3. Настоящий приказ вступает в силу с 01.01.2025.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Заместитель Председателя Правительства Ивановской области - директор Департамента здравоохранения Ивановской области **А.Е. Арсеньев**

Приложение
к приказу Департамента здравоохранения
Ивановской области
от 28.12.2024 № 247

Регламент подключения к государственной информационной системе в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области»

1. Нормативные и методические документы.

- Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 9 февраля 2022 года № 140 «О единой государственной информационной системе в сфере здравоохранения»;
- Приказ Министерства здравоохранения Российской Федерации от 24 декабря 2018 года № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»;
- Постановление Правительства Российской Федерации от 12 апреля 2018 года № 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 декабря 2017 года № 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 декабря 2018 года № 1556 «Об утверждении Положения о системе мониторинга движения лекарственных препаратов для медицинского применения»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 08 февраля 2018 года № 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 Российской Федерации от 06 июля 2015 года № 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 16 ноября 2015 года № 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 июля 2014 года № 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 июля 2018 года № 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 июля 2018 года № 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 ФСТЭК России от 18 февраля 2013 г. № 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 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении

Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

- Приказ ФСТЭК России от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

- Приказ ФАПСИ от 13 июня 2001 года № 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»;

- Методические рекомендации по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с единой государственной информационной системой в сфере здравоохранения (утв. Министерством здравоохранения РФ 14 августа 2020 г.),

2. Сокращения, используемые в регламенте

АРМ	автоматизированное рабочее место
ЛВС	локальная вычислительная сеть
ГИС СЗ РМИС СЗ ИО	государственная информационная система в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области»
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба технического и экспортного контроля Российской Федерации
СКЗИ	средства криптографической защиты информации
КИ	ключевая информация
КИИ	критическая информационная инфраструктура
Оператор	Департамент здравоохранения Ивановской области
Уполномоченная организация (УО)	Областное бюджетное учреждение здравоохранения особого типа «Медицинский информационно-аналитический центр» (ОБУЗОТ МИАЦ)
Субъекты ГИС СЗ РМИС СЗ ИО	медицинские организации государственной и частной системы здравоохранения, фармацевтические организации, организации, являющиеся соискателями лицензии на осуществление медицинской деятельности, организации, являющиеся операторами иных информационных систем, указанных в части 5 статьи 91 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

3. Общие положения

Настоящий Регламент подключения к государственной информационной системе в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области» (далее по тексту регламент) определяет и устанавливает:

- особенности подключения к ГИС СЗ РМИС СЗ ИО;
- типовые схемы подключения к ГИС СЗ РМИС СЗ ИО;
- порядок подключения к ГИС СЗ РМИС СЗ ИО;
- организацию и порядок получения и смены ключевой информации;
- порядок выполнения требований по защите информации объектов, подключаемых к ГИС СЗ РМИС СЗ ИО;
- типовые формы документов для организаций, подключаемых к ГИС СЗ РМИС СЗ ИО

Настоящий регламент обязателен к исполнению участниками информационного взаимодействия с использованием ГИС СЗ РМИС СЗ ИО и ее модулей (подсистем).

Подрядные организации, которым требуется доступ к ГИС СЗ РМИС СЗ ИО для проведения работ/оказания услуг по государственным контрактам и договорам обязаны руководствоваться настоящим регламентом на период выполнения обязательств. Подрядные организации для подключения обязаны получить письменное согласие, выдаваемое Департаментом здравоохранения Ивановской области или Уполномоченной организацией по результатам рассмотрения заявки, содержащей следующие сведения и материалы: сведения о сотрудниках, задействованных при проведения работ/оказании услуг с указанием паспортных данных сотрудников; информационных ресурсов, к которым необходим доступ с указанием обоснования с учетом предмета государственного контракта и содержания технического задания; заверенные подрядной организацией копии документов, подтверждающих выполнение требований по защите информации. Далее все подключаемые организации именуются Абонентами.

4. Назначение и задачи ГИС СЗ РМИС СЗ ИО

ГИС СЗ РМИС СЗ ИО предназначена для обработки, хранения защищаемой информации и защищенного информационного обмена.

С учетом параметров ГИС СЗ РМИС СЗ ИО в местах размещения обеспечиваются меры защиты информации, требования которых распространяются и на подключаемых Абонентов.

Цели и задачи, которые достигаются выполнением настоящего регламента:

– повышение эффективности функционирования и управления деятельностью подключаемых Абонентов;

– обеспечение информационной безопасности при передаче информации между Абонентами, в том числе информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну и персональных данных, с использованием публичных и выделенных каналов связи;

– защита от несанкционированного доступа и модификации информации в процессе информационного обмена между Абонентами и ГИС СЗ РМИС СЗ ИО;

– организация защищенных подключений для осуществления работ по модернизации, настройке и изменению программных компонентов подрядными организациями.

В ГИС СЗ РМИС СЗ ИО применяется комплексный подход к защите инфраструктуры и передаваемой информации. Защита осуществляется на всех этапах обработки информации за счет реализации мер по защите инфраструктуры и обрабатываемой им информации от несанкционированного доступа, применением межсетевого экранирования и обнаружения вторжений, как элементов системы защиты, так и подключаемых сегментов ЛВС и отдельных АРМ Абонентов, а также за счет криптографических методов защиты передаваемой информации. Все средства защиты информации, используемые в ГИС СЗ РМИС СЗ ИО, имеют действующие сертификаты ФСТЭК России и ФСБ России, либо техническую поддержку производителя средств защиты информации. Особенности функционирования систем защиты информации накладывают ограничение на перечень технических и программных средств, которые могут использовать Абоненты при подключении к ГИС СЗ РМИС СЗ ИО. Регламентом определен состав программно-технических средств и типовые схемы подключения.

Абонент, подключаемый к ГИС СЗ РМИС СЗ ИО, обязан контролировать и поддерживать в актуальном состоянии систему защиты информации от несанкционированного доступа с применением сертифицированных средств защиты информации, а также систему антивирусной защиты, на технических средствах, взаимодействующих с ГИС СЗ РМИС СЗ ИО со стороны Абонента.

5. Порядок подключения к ГИС СЗ РМИС СЗ ИО

Для подключения к ГИС СЗ РМИС СЗ ИО Абонентам определены две типовых схемы подключения. Выбор схемы определяет Уполномоченная

организация в зависимости от задач подключения и типа Абонента.

При типовых сценариях подключения для Абонентов, являющихся медицинскими организациями государственной и частной системы здравоохранения, фармацевтическими организациями, организациями, являющиеся соискателями лицензии на осуществление медицинской деятельности, организациями, являющимися операторами иных информационных систем, указанных в части 5 статьи 91 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» Регламентом определены возможными Типовые схемы №1 и №2. Для других сторонних организаций, в том числе подрядчиков и исполнителей контрактных обязательств, определена Типовая схема № 2.

Типовая схема № 1

Типовая схема № 1 представляет собой подключение в формате сегмент ЛВС Абонента к ГИС СЗ РМИС СЗ ИО. Межсетевое экранирование, в данном случае, осуществляется на границе сегмента ЛВС Абонента с использованием ПАК криптографической защиты информации. Порядок для осуществления такого подключения:

а) Абонент направляет заявку (Приложение 1) на разрешение подключения в Уполномоченную организацию с предоставлением, в том числе, сведений о соответствии подключаемой информационной системы требованиям законодательства по защите информации;

б) Уполномоченная организация после принятия положительного решения о возможности подключения направляет соответствующий документ подрядной (субподрядной) организации, предоставляющей услуги по защите информации для функционирования ГИС СЗ РМИС СЗ ИО или ее модуля (подсистемы). В запросе и разрешении должны быть описан перечень информационных ресурсов в ГИС СЗ РМИС СЗ ИО, к которым необходим доступ, а также ФИО и контактная информация лица, ответственного за подключение со стороны инициатора заявки;

в) Абонент при необходимости заключает договор с оператором сети связи;

г) Уполномоченная организация согласовывает срок подключения и доступ к точке размещения оборудования.

Типовая схема № 2

Типовая схема № 2 представляет собой подключение в формате АРМ к ГИС СЗ РМИС СЗ ИО. Подключение производится с использованием сети

Интернет. Межсетевое экранирование, в данном случае, должно осуществлятся с использованием сертифицированных средств защиты информации непосредственно на АРМ Абонента. Доступ к ГИС СЗ РМИС СЗ ИО предоставляется с использованием на АРМ специального клиентского программного обеспечения сертифицированных криптографических средств защиты информации.

Для осуществления такого подключения Абонент:

а) Абонент направляет заявку (Приложение 1) на разрешение подключения в Уполномоченную организацию с предоставлением, в том числе, сведений о соответствии подключаемой информационной системы требованиям законодательства по защите информации;

б) Уполномоченная организация после принятия положительного решения о возможности подключения направляет соответствующий документ подрядной (субподрядной) организации, предоставляющей услуги по защите информации для функционирования ГИС СЗ РМИС СЗ ИО или ее модуля (подсистемы). В запросе и разрешении должны быть описан перечень информационных ресурсов в ГИС СЗ РМИС СЗ ИО, к которым необходим доступ, а также ФИО и контактная информация лица, ответственного за подключение со стороны инициатора заявки;

в) Абонент самостоятельно приобретает, в соответствии с полученной информацией, требуемое количество программных средств защиты информации, и, получив лицензионные копии, организует за счет собственных сил и средств их установку, настройку и обслуживание подключения;

г) Абонент согласовывает сроки подключения к ГИС СЗ РМИС СЗ ИО.

д) Уполномоченная организация сообщает о готовности к защищенному информационному обмену для получения ключевой документации.

В случае наступления любого из событий, связанных с компрометацией КИ, абонент немедленно прекращает взаимодействие с ГИС СЗ РМИС СЗ ИО и сообщает о факте компрометации своему Администратору безопасности (при наличии в штате) и в Уполномоченную организацию.

Уполномоченная организация блокирует учетную запись и в порядке, предусмотренном законодательством и регламентом направляет информацию о необходимости формирования новую КИ в подрядную (субподрядную) организацию, предоставляющую услуги по защите информации для функционирования ГИС СЗ РМИС СЗ ИО или ее модуля (подсистемы). Далее УО передает файлы с новой КИ Абоненту. В зависимости от типа используемого СКЗИ, КИ может передаваться, как нарочно, так и по защищенным каналам связи.

Все действия и обязанности, специально не оговоренные настоящим Регламентом, совершаются сторонами в порядке, предусмотренном

действующим законодательством Российской Федерации и Положением о государственной информационной системе в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области».

Приложение № 1
к Регламенту

На бланке организации

_____ *(должность)* _____
Департамента здравоохранения
Ивановской области
_____ *(И.О. Фамилия)*____

Исх. № _____
__.__.20__г.

Уважаемый(ая) _____!

Просим согласовать предоставление удаленного доступа к ресурсам государственной информационной системы в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области» сотрудникам _____ *(наименование организации)* для выполнения [работ и/или услуг], предусмотренных _____ [*реквизиты документа, на основании которого требуется доступ*].

Соблюдение всех требований действующего законодательства по организации защиты информации при [проведении работ и/или оказании услуг] подтверждаем приложенными к заявке документами.

Приложение: заявка на предоставление доступа – на ____ л.

должность _____ *И.О. Фамилия*

На бланке организации

_____ *(должность)* _____
Департамента здравоохранения
Ивановской области
_____ *(И.О. Фамилия)*____

Исх. № _____
__.__.20__г.

ЗАЯВКА
НА ПРЕДОСТАВЛЕНИЕ ДОСТУПА К РМИС СЗ ИО

_____ *(наименование организации)*, в лице _____ *(должность, ФИО)*, на основании _____ *(реквизиты документа)*, просит предоставить удаленный доступ к [тестовому контуру (ландшафту), ландшафту разработки (доработки) или подсистем(ы) _____ *(указать)*] государственной информационной системы в сфере здравоохранения «Региональная медицинская информационная система системы здравоохранения Ивановской области» (далее – ГИС РМИС СЗ ИО) для проведения работ _____ в соответствии с положениями _____ *(указать раздел и/или пункт из документа, указывающий на необходимость проведения работ и/или услуг)*.

Дата и время проведения работ: с __.__.20__г. по __.__.20__г.

[Место подключения для ведения удаленных работ: _____.]

Для проведения работ уполномочены лица:

№ п/п	ФИО лица	Должность	Полномочия	Контактные данные (e-mail, номер телефона)	Срок предоставления доступа
1.					
2.					
3.					

Настоящим подтверждаем, что согласны с тем, что при несоответствии действий с нашей стороны заявленным работам и/или при возникновении подозрительной активности на ресурсах ГИС СЗ РМИС СЗ ИО в ходе работ, контролирующие работы технические специалисты Уполномоченной организации, вправе приостановить доступ до прояснения ситуации или получения иной заявки, оформленной надлежащим образом.

Приложения:

1) паспортные данные (данные документа, удостоверяющего личность) *(фамилия, имя, отчество, дата рождения, серия и номер документа, удостоверяющего личность, кем выдан, когда, место регистрации)* или копия паспорта/ документа, удостоверяющего личность каждого уполномоченного лица;
2) техническая карта работ, содержащая *(не менее)*:
   a) подробный перечень планируемых работ, с указанием последовательности выполнения операций и нормы отведенного времени на каждую операцию;
   b) перечень оборудования, инструментов, разновидности и количество расходных материалов, которые будут использоваться при работах;
3) выписка из трудовой книжки или ее копия (при необходимости);
4) соглашение о конфиденциальности;
5) лист ознакомления всех уполномоченных работников с соглашением о конфиденциальности;
6) _____ (иное, при необходимости).

Дата _____

должность _____ *И.О. Фамилия*

СОГЛАШЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ № _____

г. Иваново

_____20__г.

Департамент здравоохранения Ивановской области в лице _____, действующего на основании _____ с одной стороны

и

_____, в лице _____, действующего на основании _____, с другой стороны,

вместе именуемые «Стороны»,

руководствуясь принципами соблюдения условий гарантированной защиты информации ограниченного доступа, не использования ее во вред друг другу, стремясь не допускать распространения информации ограниченного доступа, Стороны заключили настоящее Соглашение о нижеследующем.

Статья 1.

1.1. Настоящее соглашение регулирует отношения между Сторонами, по обработке информации, полученной в ходе исполнения Государственного контракта от __.__.20 г. № _____ на _____ (далее - Контракт).

1.2. Условия настоящего Соглашения не распространяются на информацию, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

1.3. Стороны договорились использовать в настоящем Соглашении следующие термины:

Аффилированные Лица - взаимосвязанные структуры, любое физическое или юридическое лицо, которое прямо или опосредованно могут влиять друг на друга при принятии решений;

Доступ к информации ограниченного доступа - ознакомление определенных лиц с информацией, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

Информация ограниченного доступа - информация, содержащая сведения конфиденциального характера, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информацией ограниченного доступа не является:

- свободно распространяемая информация;
- общеизвестные сведения и иная информация, доступ к которой не ограничен;
- которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информация, в отношении которой Получающая Сторона и/или ее Аффилированные или Уполномоченные Лица могут доказать, что она была им известна до раскрытия Раскрывающей Стороной и/или ее Уполномоченными Лицами;

Обработка информации — совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с конфиденциальной информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), удаление и уничтожение;

Передача информации ограниченного доступа - передача информации ее обладателем контрагенту на основании договора в объеме и на условиях, которые

предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

Получающая сторона – Сторона Соглашения, получающая конфиденциальную информацию и принимающая на себя обязательства по защите информации для обеспечения сохранности ее конфиденциальности самой Получающей стороной, ее Аффилированными и Уполномоченными лицами всеми необходимыми мерами, предусмотренными действующим законодательством РФ, правилами делового оборота и/или настоящим Соглашением;

Предоставление информации - действия, направленные на раскрытие информации определенному лицу или определенному кругу лиц;

Распространение информации - действия, направленные на раскрытие информации неопределенному кругу лиц;

Раскрывающая сторона – Сторона Соглашения, передающая информацию;

Сведения конфиденциального характера - сведения:

- о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);
- связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);
- о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

Уполномоченные Лица - директора, должностные лица или работники Стороны и/или ее Аффилированных Компаний, или приглашенные специалисты такой Стороны и/или ее Аффилированных Компаний, которым требуется доступ к Конфиденциальной информации в связи с исполнением Контракта.

1.4. Настоящий документ представляет собой полное Соглашение, заключенное между сторонами в отношении обмена и защиты информацией ограниченного доступа.

1.5. Настоящее Соглашение регулируется и толкуется в соответствии с законодательством Российской Федерации.

1.6. Изменения и дополнения к настоящему Соглашению могут быть внесены только на основании письменного соглашения, подписанного должным образом уполномоченными представителями сторон.

1.7. Настоящее Соглашение не предусматривает какое-либо предоставление прав интеллектуальной собственности, включая авторские права, товарные знаки, а также право на изготовление, заказа на изготовление, использование или продажу Конфиденциальной информации.

Статья 2.

2.1. Стороны обязуются использовать взаимно предоставленную или ставшую известной в ходе взаимодействия информацию ограниченного доступа (далее - Информацию) только и исключительно в целях реализации задач в рамках исполнения Контракта, при этом обязуются обеспечить ее хранение с принятием соответствующих мер, предусмотренных законодательством Российской Федерации по ее защите за исключением случаев, когда обязанность такого раскрытия установлена требованиями закона или вступившим в законную силу судебным решением.

Информация может быть предоставлена лицам, не участвующим в исполнении Контракта исключительно в объеме, указанном в мотивированном запросе уполномоченного на то государственного либо иного органа в пределах его полномочий, если обязанность по ее раскрытию прямо установлена законом.

2.2. Получающая сторона имеет право предоставить Информацию своим Аффилированным Лицам без предварительного письменного согласия Раскрывающей Стороны, только если указанная Информация необходима для исполнения Контракта и при условии, что предварительно Получающая Сторона заключит с каждым из таких лиц соглашение о конфиденциальности на тех же условиях, что и настоящее Соглашение.

2.3. Для защиты Информации Получающая сторона должна принимать меры технического и организационного характера, предусмотренные российским законодательством.

2.4. При условии выполнения требований п. 2.3. настоящей статьи Соглашения Получающая сторона не должна нести ответственность за раскрытие Информации в следующих случаях:

- если раскрытие Информации произошло при наличии предварительного согласия Раскрывающей стороны, оформленного в письменном виде;
- если раскрытие Информации произошло в соответствии с актом (решением) суда и/или государственного либо иного органа, с учетом положений п.2.1 настоящего Соглашения.

2.5. В случае, если Информация является собственностью одной из Сторон, то она, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к Информации, определять порядок и условия такого доступа;

2) использовать Информацию, в том числе распространять ее, по своему усмотрению;

3) передавать Информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения Информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с Информацией или разрешать осуществление таких действий.

2.6. Передача Информации по каналам связи без принятия мер защиты, соответствующих требованиям российского законодательства, запрещена.

Статья 3.

3.1. Настоящее Соглашение вступает в силу с даты его подписания. Действие Соглашения прекращается по истечении 5 (пяти) лет после исполнения Контракта.

3.2. В случае прекращения переговоров по вопросам, связанным с выполнением Контракта и/или прекращения исполнения любой из Сторон Контракта, настоящее Соглашение действует в течение 5 (пяти) лет с даты его подписания, независимо от возврата, уничтожения Информации и каких-либо ее копий.

3.3. В случае реорганизации одной из Сторон настоящего Соглашения обязанность по защите Информации, а также ответственность за его нарушение (включая обязанность по возмещению убытков) переходит к правопреемнику реорганизованной стороны.

3.4. В случае ликвидации одной из Стороны она обязана до завершения ликвидации вернуть другой стороне все оригиналы и копии всех материальных носителей Информации.

Статья 4.

4.1. Стороны не дают никаких подтверждений или гарантий, явных или подразумеваемых, в отношении качества, достоверности, точности и полноты информации, раскрываемой в соответствии с настоящим Соглашением.

4.2. Одновременно стороны признают и допускают возможность наличия в информации, передаваемой в соответствии с настоящим соглашением, ошибок и неточностей.

Статья 5.

5.1. Стороны несут ответственность в соответствии с действующим российским законодательством за действия всех своих сотрудников, Аффилированных и/или Уполномоченных лиц, а также приглашенных ими специалистов для исполнения Контракта, приведшие к распространению Информации.

5.2. Сторона обязана незамедлительно сообщить обладателю Информации о допущенном либо ставшем ему известном факте распространения, разглашения или угрозы разглашения, незаконном получении или незаконном использовании указанной Информации третьими лицами.

Статья 6.

6.1. Стороны обязуются добросовестно путем переговоров разрешать все претензии, споры, противоречия или разногласия, которые могут возникнуть между ними в отношении или в связи с настоящим Соглашением, или исполнением, нарушением, прекращением или недействительностью данного Соглашения. Однако, если Стороны окажутся не в состоянии достичь согласия, то все претензии, споры, противоречия и разногласия подлежат урегулированию в Арбитражном суде г. Иваново.

Статья 7.

Департамент здравоохранения Ивановской области
Адрес (юридический и почтовый): 153000, г. Иваново, пр. Шереметевский, д. 1.
ИНН 3729010595, КПП 370201001, ОГРН 1023700535088,
Адрес электронной почты:_____; Телефон: _____

__*(наименование Стороны)*_____
Адрес (юридический и почтовый):_____ _____
ИНН: _____, КПП: _____, ОГРН(ОГНИП): _____
Адрес электронной почты:_____; Телефон: _____

Департамент здравоохранения Ивановской области	***Наименование Стороны***
Должность руководителя	*Должность руководителя*
_____/ *И.О. Фамилия*	_____ / *И.О. Фамилия*
М.П.	М.П.

ЛИСТ ОЗНАКОМЛЕНИЯ

с положениями соглашения о конфиденциальности

Мы, нижеподписавшиеся, подтверждаем, что внимательно изучили положения соглашения о конфиденциальности от __.__.20__ г. № _____, заключенного между **Департаментом здравоохранения Ивановской области** и _____ и обязуемся соблюдать его требования при [выполнении работ или оказании услуг], предусмотренных _____ *(основание работ: реквизиты контракта, договора, пр.)*.

№ п/п	Фамилия И.О.	Должность	Дата ознакомления
1			
2			
3			
4			
5			
5			
6			
7			