федеральное государственное бюджетное
образовательное учреждение высшего образования
«Самарский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО СамГМУ Минздрава России)

УТВЕРЖДЕНО
Приказом Ректора
член-корреспондента РАН
з.д.н. РФ
А.В. Колсанова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7A6B8A5E9CB221443586B1F30109C6F1
Владелец: Колсанов Александр Владимирович
Действителен: с 02.04.2026 до 26.06.2027

РЕГЛАМЕНТ № 5П/08-31-2026
обеспечение защиты информации при взаимодействии с подрядными организациями в ФГБОУ ВО СамГМУ Минздрава России

Приложение № 5
к приказу ректора ФГБОУ ВО
СамГМУ Минздрава России
№ 169 от 31.08.2026 г.

Самара 2026

1. Общие положения

1.1. Предметом настоящего Регламента является утверждение порядка совместных действий по организации взаимодействия между ФГБОУ ВО СамГМУ МЗ РФ и подрядной организацией. Взаимодействие может осуществляться как с обеспечения обмена электронными документами, связанными с передачей персональных данных, служебной и другой конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, по телекоммуникационным каналам связи на основе технологии ViPNet (ЗСПД), так и без подключения к телекоммуникационным каналам связи.

1.2. Настоящий Регламент разработан в соответствии со следующими руководящими документами:

- 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 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- письмо ФСТЭК России от 07.10.2025 № 240/92/3228 «О мерах по повышению защищенности информационной инфраструктуры Российской Федерации».

2. Организационные требования

2.1. Организация обмена электронными документами осуществляется путем отправки и получения документов (договоров) между сервисами документооборота, таких как СБИС, ДИАДОК и.т.д.

2.2. В срок, не позднее 5 (пяти) рабочих дней с даты заключения Контракта (Договора/Соглашения) с подрядной организации подписывается Соглашение. В случае если у подрядной организации нет необходимости подключения к ЗСПД оформляется Обязательство о соблюдении конфиденциальности защищаемой информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну по форме, определенной в Приложении к настоящему регламенту. В случае если есть необходимость подключения подрядной сети к ЗСПД Университета, то

оформляется соглашение о межсетевом взаимодействии ViPNet-сетей к защищенной сети ViPNet СамГМУ форма которого утверждена в «Регламенте подключения к защищенной сети передачи данных ViPNet №14369 ФГБОУ ВО СамГМУ Минздрава России»

2.3. При необходимости Стороны подключиться к ЗСПД за свой счет приобретают, устанавливают и обеспечивают работоспособность программных и технических средств, СКЗИ, необходимых для работы в ЗСПД, а также самостоятельно и независимо друг от друга несут расходы, связанные с эксплуатацией программных и технических средств, СКЗИ, средств и каналов связи, необходимых для работы в ЗСПД.

2.4 В случае необходимости подключения к ЗСПД направляется Заявка на подключение к ЗСПД, подписанная руководителем заявителя в адрес УИБ СамГМУ (адрес 443099, г. Самара, ул. Чапаевская, 89 каб. 103, эл.почта cib@samsmu.ru). В зависимости от типа подключения к ЗСПД к заявке необходимо приложить данные согласно Регламента подключения к защищенной сети передачи данных ViPNet №14369 ФГБОУ ВО СамГМУ Минздрава России утверждённым Приказом Ректора № 259 от 28.12.2024 «Об утверждении Инструкций и регламентов».

2.5 Работникам подрядных организаций предоставляется доступ только к тем ресурсам и информации, которые необходимы для выполнения конкретных задач

2.6. В срок, не позднее 10 (десяти) рабочих дней с даты заключения Контракта (Договора/Соглашения) стороны должны ознакомиться со следующими нормативными документами:

1) Политики информационной безопасности
2) Политика в отношении обработки ПДн
3) Инструкции пользователей средств криптографической защиты информации»
4) Регламент подключения к защищенной сети ViPNet СамГМУ
5) Инструкция по использованию персонального компьютера и ресурсов сети СамГМУ
6) Регламент выявления инцидентов информационной безопасности и реагирование на них в ФГБОУ ВО СамГМУ Минздрава России

2.7. Подрядная организация должна предоставить список работников организации, привлекаемых к оказанию услуг (выполнению работ), в формате официального письма путем направления заказного письма с уведомлением о вручении или по защищенным каналам связи с использованием ЗСПД.

2.8. В случае работы с ПД от этих сотрудников должны быть получены согласия на обработку персональных.

2.9. В случае изменения состава работников подрядной организации, привлекаемых к оказанию услуг (выполнению работ), в течении 2 календарных дней уведомляет о факте таких изменений путем направления заказного письма с уведомлением о вручении, передачи нарочно уполномоченному работнику или по защищенным каналам связи с использованием ЗСПД.

2.10. Работникам подрядных организаций должны незамедлительно информировать о фактах произошедших компьютерных атак и компьютерных инцидентов в информационной инфраструктуре подрядной организации в период оказания услуг (выполнения работ).

3. Требования к средствам защиты информации

3.1. Требования к средствам защиты информации при подключении подрядных организаций к ЗСПД и информационным системам Университета регламентирован Приказом Ректора № 259 от 28.12.2024 «Об утверждении Инструкций и регламентов» приложением 4 Регламент подключения к защищенной сети передачи данных ViPNet №14369 ФГБОУ ВО СамГМУ Минздрава России.

3.2. Требования к АРМ подрядной организации

3.2.1. Подключение с АРМ из информационной инфраструктуре подрядной организации разрешено только при использовании СКЗИ VipNet Client сети №14369.

3.2.2. Наличие на АРМ сертифицированных по требованиям безопасности информации ФСТЭК России средств антивирусной защиты.

3.2.3 Наличие сертифицированных по требованиям безопасности информации ФСТЭК России средств защиты от несанкционированного доступа. Допускается применение средств защиты от несанкционированного доступа в составе сертифицированной по требованиям безопасности информации ФСТЭК России операционной системы.

3.2.4. Реализован в информационной инфраструктуре подрядной организации защиты почтовых сервисов от фишинга.

3.2.5 Реализован в информационной инфраструктуре подрядной организации мониторинг сетевых атак и вредоносного ПО в файлах, передаваемых в сетевом трафике.

3.2.6 Требования, указанные в настоящим разделе, подрядная организация реализует своими силами и средствами, без дополнительных затрат со

стороны Университета.

4. Требования к безопасности АРМ и ресурсам Университета

4.1. Работникам подрядных организаций предоставляется доступ только к тем ресурсам и информации, которые необходимы для выполнения конкретных задач. Учётные записи и рабочие места (АРМ) ограничиваются доступом к определённым серверам и информационным ресурсам.

4.2 Пароли от учётных записей информационных ресурсов Университета выдаются под роспись в журнале «Выдачи парольной документации».

4.3. Полученные данные в информационных ресурсах Университета данные должны использоваться персонально каждым работником подрядной организации без передачи третьим лицам.

4.4. Данные не должны использоваться работниками подрядной организации после завершения оказания услуг и гарантийных обязательств и подлежат уничтожению подрядной организацией.

5. Контроль за информационной безопасностью при работе с подрядными организациями

5.1. Контроль за информационной безопасностью при работе с подрядными организациями осуществляется специалистами информационной безопасности. Проверки подрядных организаций в направлении информационной безопасности могут проводиться как в плановом, так и внеплановом режиме.

5.2. Для проведения контроля за информационной безопасностью при работе с подрядными организациями могут привлекаться руководители подрядных организаций.

5.3 С целью контроля за информационной безопасностью могут проходить Проверки. Проверки могут быть как плановые так и не плановые Плановая проверка подрядчика проводится совместно с представителем подрядчика.

5.4. Внеплановые проверки подрядных организаций проводятся:

- по результатам устранения нарушений, выявленных при плановой проверке;
- при проведении проверок информационной безопасности;
- по информации о фактах нарушения требований обработки информации подрядной организации;

5.5. При проведении проверки подрядной не менее чем за 2 (два) рабочих дня направляется в адрес подрядной организации письменное уведомление.

5.6. По результатам проверок оформляется и регистрируется акт о выявленных нарушениях требований информационной безопасности. В

случае зафиксированных нарушений настоящего Порядка, Университет вправе приостановить доступ подрядной организации к своим информационным активам.

5.7. Для восстановления доступа в адрес Университета направляются документы, свидетельствующие о факте устранения выявленных нарушений. Решение о возобновлении доступа подрядной организации к информационным активам принимается Ректором Университета после изучения предоставленных документов.

5.8. В случае возникновении компьютерного инцидента в информационной инфраструктуре подрядной организации в период оказания услуг (выполнения работ), приведшего к нарушению конфиденциальности, целостности и доступности информации Университета, ответственность за последствия возникшего компьютерного инцидента несет подрядная организация.

5.9. В ходе всего срока выполнения работ по договору рекомендуется проводить совещания с представителями подрядной организации в рамках которого рассматриваются вопросы в области информационной безопасности. На совещаниях рассматриваются текущие вопросы в области информационной безопасности, выявленные нарушения, действия по их устранению/предотвращению нарушений. Совещание может проводиться как в очном, так и в онлайн формате.

Приложение к регламенту
от «___» _____20___ г. № ____

Обязательство о соблюдении конфиденциальности защищаемой информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну

Я, _____ ,
(фамилия, имя, отчество)

работающий(ая) в должности _____
_____
_____
_____
(должность, наименование структурного подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к защищаемой информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация). Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам защищаемую информацию, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня защищаемую информацию, сообщать непосредственному руководителю.
3. Не использовать защищаемую информацию с целью получения выгоды.
4. Выполнять требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации.
5. После расторжения со мной служебного контракта (трудового договора) не разглашать и не передавать третьим лицам известную мне защищаемую информацию.

Я предупрежден(а) о том, что в случае разглашения мной защищаемой информации или ее утраты я несу ответственность, предусмотренную действующим законодательством.

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)