Чек-лист проверки подрядчиков по 152-ФЗ

Пройдите по каждому подрядчику из карты медданных: классифицируйте, сверьте условия поручения по ст. 6 ч. 3 152-ФЗ, проверьте охват договора и заведите строку реестра. Инженерные рекомендации, не юридическая консультация.

1. Классификация подрядчика – ст. 3 и 6 152-ФЗ

- [ ] Хранит или видит ПДн пациентов в целях клиники → обработчик: договор по ст. 6 ч. 3
- [ ] Свои цели и основание (страховщик ДМС, платёжный сервис) → самостоятельный оператор
- [ ] Иностранное лицо или базы за рубежом → стоп для медданных (ст. 18 ч. 5, ст. 12, ст. 6 ч. 6)

2. Обязательные условия поручения – ст. 6 ч. 3

- [ ] Перечень ПДн, перечень действий с ними и цели обработки
- [ ] Конфиденциальность и неразглашение врачебной тайны (ст. 13 323-ФЗ), роли с доступом
- [ ] Хранение в базах на территории РФ (ст. 18 ч. 5) и меры по ст. 18.1
- [ ] Защита по ст. 19: уровень защищённости, меры приказа ФСТЭК № 21, СКЗИ
- [ ] Уведомление оператора об инцидентах (ч. 3.1 ст. 21) – срок в часах
- [ ] Документы о соблюдении требований по запросу, в том числе до начала обработки
- [ ] По договору: субподрядчики с согласия оператора; возврат и уничтожение (ст. 21)

3. Пять проверок, прежде чем полагаться на договор

- [ ] Охват: сервис, аттестованный сегмент и регион хранения в РФ названы письменно
- [ ] Настройка по модели угроз: аттестат провайдера не покрывает ваше приложение
- [ ] Уведомление – в часах: у оператора 24 ч на РКН, у значимого объекта КИИ – 3 ч
- [ ] Расторжение: выгрузка оператору, удаление по репликам и бэкапам, акт об уничтожении
- [ ] ИИ: без обучения на ваших данных, обработка и логи в РФ, охват конкретного API

4. Тревожные признаки – остановиться и исправить

- [ ] Зарубежный SDK аналитики в контуре с медданными; записи на личном диске сотрудника
- [ ] Напоминания со специальностью или диагнозом через шлюз без поручения
- [ ] Субподрядчик, о котором не знает оператор; договор согласован, но не подписан

5. Реестр подрядчиков – одна строка на подрядчика

- [ ] Подрядчик, страна юрлица · данные и действия · цель · регион и сегмент · договор (дата)
- [ ] Согласие оператора · срок уведомления, ч · субподрядчики · запрос документов · удаление