Гид по решению: E2EE в телемедицине

Транспортное шифрование WebRTC уже закрывает инженерную задачу канала. Выбирайте E2EE, только если выполнено условие из раздела А и вы готовы оплатить раздел В. Вопрос о СКЗИ – отдельный (раздел С). Инженерные рекомендации, не юридическая консультация.

А. Когда E2EE оправдан

- [ ] Особо чувствительная помощь: психиатрия, психотерапия, наркология – где утечка катастрофична
- [ ] Медиаплоскость у подрядчика, которой вы не до конца доверяете (поручение и РФ всё равно нужны)
- [ ] Заказчик пишет E2EE в ТЗ – уточните, не имеет ли он в виду СКЗИ или «шифрование везде»
- [ ] Нужно снизить риск изнутри: серверы и персонал не должны видеть консультации
- [ ] Иначе транспортного шифрования достаточно: профилактике и наблюдению E2EE не нужен

Б. Чего E2EE стоит

- [ ] Запись на сервере прекращается – пишите на точке или через названный комплаенс-рекордер
- [ ] Транскрипция и ИИ-помощник врача на сервере отключаются – только на устройстве
- [ ] Старые телефоны и браузеры без RTCRtpScriptTransform – нужен запасной вариант
- [ ] Ключи – ваша задача: раздача и ротация (MLS); потеря ключа = потеря данных
- [ ] Отладка и поддержка дороже; без сверки ключей гарантия «сквозного» слабеет

В. E2EE и ГОСТ – разные вопросы

- [ ] Если модель угроз закрывает угрозу криптографией – нужны СКЗИ ФСБ нужного класса (приказ № 378)
- [ ] SFrame на AES в браузере – не ГОСТ и не СКЗИ; самописный «Кузнечик» – тоже не СКЗИ
- [ ] Требование СКЗИ обычно закрывают на каналах: ГОСТ-VPN, ГОСТ-TLS на шлюзах и в канале с МИС

Г. Правило честного заявления

- [ ] Спросите: «могут ли наши серверы технически видеть медиа?» Если да – это не сквозное шифрование
- [ ] Спросите: «какое СКЗИ, какой сертификат, какой класс?» Нет ответа – не пишите «по ГОСТ»
- [ ] Запись при E2EE – один названный, журналируемый рекордер в вашем контуре в РФ, с информированием