Чек-лист перед стартом WebRTC-телемедицины

Пятнадцать проверок до первого спринта: бюджет TURN, проблемные сети, граница медданных, запись, топология. Пройдитесь по своей архитектуре, затем по каждому предложению вендора. Инженерные рекомендации, не юридическая консультация.

1 · TURN и сетевой бюджет

- [ ] TURN развёрнут со своими учётными данными – никаких публичных реле из учебных примеров
- [ ] Доля реле задана (база 5–20%, в больничных сетях выше); ГБ/мес – в модели стоимости
- [ ] Реле стоят в России, рядом с пациентами; цена гигабайта у провайдера известна

2 · Проблемные сети

- [ ] Лестница фолбэков проверена: UDP → TURN/UDP → TURN/TCP → TURN/TLS на 443
- [ ] Техпроверка идёт в виртуальной приёмной, пока пациент ещё может сменить сеть
- [ ] Пилот проверен на больничном Wi-Fi, мобильном CGNAT и сельском интернете

3 · Граница медданных – 152-ФЗ, ПП 1119, приказ ФСТЭК № 21

- [ ] Каждый сервер в пути медиа (TURN, SFU, записи) – в России: свой или по поручению
- [ ] ЕСИА-вход, журналы и контроль доступа – вокруг звонка: шифрование ≠ комплаенс
- [ ] Решение о СКЗИ записано в модели угроз; нет медданных в сигналинге, URL комнат и логах

4 · Решение о записи

- [ ] Писать или нет – решено в первую неделю: от этого зависят топология и вендоры
- [ ] Если пишем: сервер, шифрование при хранении, доступ, хранение 1 год (193н), согласие
- [ ] Планы на сквозное шифрование сверены с записью – они конфликтуют; выбор осознанный

5 · Топология и масштаб

- [ ] SFU заложен для любой сессии, где возможен третий: переводчик, родственник, второй врач
- [ ] Для 1:1 осознанно выбран P2P или SFU (телеметрия и запись против цены сервера)
- [ ] Реконнект и аудиорежим в приложении описаны; телефонная линия – только поддержка

Пять вопросов вендору

- [ ] Какая доля сессий идёт через TURN и где стоят ваши реле? Что происходит в сети, где закрыт UDP?
- [ ] Подпишете поручение на TURN, SFU и хранилище записей? Где лежат записи и у кого ключи? Что меняется, когда подключается третий участник?