Референсная архитектура телемедицины по 152-ФЗ и 323-ФЗ

Fora Soft Learn

Граница медданных телемедицинского видеостека в российской инфраструктуре: свои компоненты и подрядчики по поручению, шифрование соединений, сегментация плоскостей, неизменяемый журнал событий; снаружи – периферия без доступа к медданным.



ШЕСТЬ ПРАВИЛ – отметьте, что уже есть

- ☐ **Сначала проведите границу медданных.** Проследите каждый поток, включая логи, краш-репорты и SDK; карта – основа модели угроз и уровня защищённости по ПП 1119.
- ☐ **Только три вида компонентов.** Свои, подрядчики по поручению (ст. 6 ч. 3 152-ФЗ) с серверами в РФ или «слепые»; хранение зашифрованных медданных – тоже обработка.
- ☐ **Шифруйте каждое соединение и хранилище; ключи – отдельно.** DTLS-SRTP для медиа, TLS 1.2/1.3 везде, включая внутренние соединения, конвертное шифрование через KMS, секреты – в менеджере; СКЗИ, где модель угроз опирается на криптографию.
- ☐ **Сегментируйте четыре плоскости.** Медиа / приложение / данные / админ, переходы – запрет по умолчанию; перечень переходов – схема информационных потоков для модели угроз.
- ☐ **Журнал – сквозной сервис.** Неизменяемый, hash-цепочка, отдельные учётки, синхронные часы; логи – тоже медданные и хранятся внутри границы (ст. 19 ч. 2 п. 8).
- ☐ **Медданные не утекают на периферию.** Никаких идентификаторов в логах, URL, аналитике, push, тикетах поддержки и случайных бэкапах; зарубежные SDK и API к медданным не подпускать.

Плюс слой 323-ФЗ: ЕСИА для участников, ФРМР и ФРМО, УКЭП врача, ФЭР и РЭМД за 1 рабочий день. Раз в квартал – самоаудит за пять минут из статьи; статус проекта замены приказа ФСТЭК № 21 перепроверяйте (на 24.09.2026 не подписан). Инженерные рекомендации, не юридическая консультация.