Чек-лист шифрования для телемедицины

Проходите перед запуском и перед каждой проверкой. Зашифровано – не значит законно: нужны ещё поручение, локализация и контроль доступа. Не юридическая консультация.

1 · При передаче – ст. 19 152-ФЗ, группа ЗИС приказа ФСТЭК № 21

- [ ] Медиа WebRTC только на DTLS-SRTP (RFC 8827) – нигде нет самодельного открытого транспорта
- [ ] TLS 1.2+, лучше 1.3, на сигналинге, API и вебхуках; связи сервис-сервис – TLS или mTLS
- [ ] SFU расшифровывает медиа: в России, внутри границы медданных, под поручением
- [ ] Никаких медданных в SMS, письмах и push: эти каналы не под вашим контролем

2 · При хранении – ст. 19 ч. 2 п. 5 152-ФЗ, группа ЗНИ

- [ ] В инвентаре все хранилища: записи, транскрипты, чат, сигналинг, логи, бэкапы, устройства
- [ ] Объекты – серверное шифрование + ключ KMS (конверт); базы – TDE или шифрование тома
- [ ] Ноутбуки и телефоны – полнодисковое шифрование через MDM, а не через памятку
- [ ] Бэкапы и выгрузки – та же дисциплина ключей; списание – уничтожение или крипто-стирание

3 · ГОСТ и СКЗИ – приказ ФСБ № 378

- [ ] Модель угроз по каждому участку: закрыто без криптографии или нужен СКЗИ – письменно
- [ ] Где нужен СКЗИ – сертифицированное средство; WebRTC и облачный AES им не являются
- [ ] Каналы с МИС клиники и между площадками – ГОСТ-TLS или ГОСТ-VPN, если так решила модель
- [ ] СКЗИ в уведомлении РКН (ст. 22 ч. 3 п. 7) = модель угроз = конфигурация в продакшене

4 · Ключи – опора всех слоёв

- [ ] Конвертное шифрование через KMS; каждый вызов ключа авторизован и попадает в журнал
- [ ] Ключи и данные в разных доменах отказа – не на одном диске, в репозитории или аккаунте
- [ ] Владелец корневого ключа письменно: провайдер / CMK / HSM или СКЗИ / устройство (E2EE)

5 · Утечка и тревожные признаки – ст. 21 ч. 3.1 152-ФЗ

- [ ] Исключения «зашифровано – не утечка» нет: РКН за 24 и 72 ч, доказательства ключей готовы
- [ ] Тревожный признак: вечные подписанные ссылки; TLS 1.0/1.1 там, куда ходит пациент или МИС
- [ ] Тревожный признак: обещано E2EE, а запись, транскрипция или ИИ работают на сервере

Рабочая таблица – одна строка на хранилище, храните рядом с моделью угроз

- [ ] Хранилище _____ · механизм _____ · ключ _____ · СКЗИ да/нет · ключ отдельно ✓/✗ · владелец ____