Чек-лист аудит-журналов для телемедицины

Прогоняйте перед запуском и перед каждой проверкой: журнал, который никто не разбирает, – улика против вас. Инженерные рекомендации, не юридическая консультация.

А. Журналируйте события – ст. 19 ч. 2 п. 8 152-ФЗ, РСБ.1–РСБ.2

- [ ] Входы (успех и отказ, метод: ЕСИА, SSO, 2FA), выдача ролей, вход поддержки «от имени»
- [ ] Зал ожидания: постановка в очередь, допуск (кем), отказ, перевод к другому врачу
- [ ] Сессия: вход и выход участника с ролью, смена ролей, демонстрация экрана, чат без текста
- [ ] Запись и транскрипт: старт по согласию, каждый просмотр, скачивание, удаление по сроку
- [ ] Медкарта, подпись УКЭП и передача ЭМД в РЭМД, конфигурация журнала, break-glass

Б. Контроль доступа – ИАФ и УПД приказа ФСТЭК № 21

- [ ] Уникальный ID везде – никаких общих логинов в регистратуре и на постах (ИАФ.1, ИАФ.3)
- [ ] Участники – через ЕСИА; врач – в ФРМР, документы консультации подписаны его УКЭП
- [ ] Матрица «роль + лечебное отношение» записана; переводчик ограничен сессией (УПД.4–5)
- [ ] Поддержка – по времени, с тикетом и причиной; второй фактор у персонала и админов
- [ ] Блокировка сеанса по типу рабочего места (УПД.10); увольнение – блок в тот же день

В. Защитите журнал – РСБ.3, РСБ.6, РСБ.7

- [ ] В событиях ссылки, а не медданные: без текста чатов, диагнозов и подписанных ссылок
- [ ] Журнал – медданные: шифрование, хранение в России, доступ по служебной необходимости
- [ ] WORM со строгой блокировкой объектов + цепочка хэшей; прод не может писать и удалять
- [ ] Синхронизация времени всех сервисов; алерт на сбои и разрывы в потоке событий (РСБ.4)
- [ ] Подрядчик журнала – по поручению (ст. 6 152-ФЗ); никаких зарубежных SaaS для логов

Г. Хранение и разбор – РСБ.1, РСБ.5, п. 17 ПП 1119

- [ ] Документ по РСБ.1: перечень событий и сроки хранения – срок выбирает оператор
- [ ] Ориентир: события безопасности – от 3 лет; доступ к ЭМД – не меньше срока ЭМД
- [ ] Уничтожение ПДн: акт + выгрузка из журнала, хранить 3 года (приказ РКН № 179)
- [ ] Алерты → разбор раз в неделю → break-glass раз в месяц → пересмотр доступа раз в квартал
- [ ] Каждый разбор оставляет подписанный след; итоги расследования для РКН – за 72 часа