# Чек-лист аудита утечек медданных

Для телемед-продукта: проверяйте перед запуском и после каждого нового SDK, подрядчика или шаблона уведомлений. Десять ошибок в четырёх группах; каждый неотмеченный пункт может обернуться инцидентом с 24 часами на уведомление Роскомнадзора. Инженерные рекомендации, не юридическая консультация.

## 1. Где лежат данные – 152-ФЗ ст. 12, ст. 18 ч. 5

- [ ] Инвентарь внешних сервисов собран по исходящему трафику, а не по памяти команды
- [ ] Ни одна база с медданными не лежит за рубежом: SaaS, хелпдеск, CRM, трекер ошибок, формы
- [ ] Чат с пациентами – внутри продукта (ЕСИА, журнал); личные мессенджеры запрещены политикой
- [ ] ИИ-функции – российский провайдер по поручению или модель on-prem; зарубежных ИИ-API нет

## 2. Медданные не на своём месте – ст. 5, 19, ст. 21 ч. 3.1

- [ ] URL без пациента и диагноза: непрозрачные ID, данные в теле POST, Referrer-Policy: no-referrer
- [ ] Логи и краш-репорты – только ID и коды; очистка включена; стек логов в российском контуре
- [ ] Тестовые среды – синтетика или обезличенная выгрузка, а не копия продакшена
- [ ] Внешняя аналитика и пиксели – только на публичном сайте; в продукте – свой конвейер
- [ ] Push, SMS и письма без специальности, анализов и диагноза; контент – в приложении после входа
- [ ] Записи: запрет публичного доступа для всей организации, KMS, подписанные ссылки, журнал

## 3. Документы – 152-ФЗ ст. 6, 9, 10, 22

- [ ] Согласие – отдельный документ под каждую цель: версия, время подписи, поток отзыва
- [ ] Уведомление РКН подано до начала обработки; изменения – до 15-го числа следующего месяца
- [ ] Реестр поручений: у каждого подрядчика с медданными – поручение и данные в РФ

## 4. Клиника и инциденты – 193н п. 38–40, ст. 21 ч. 3.1

- [ ] Без очного приёма по обращению – заключение без поля диагноза и без кнопки рецепта
- [ ] Регламент на 24/72 часа отработан на учениях; доступ к порталу ПДн есть; сроки подрядчиков – в часах
- [ ] Доступ отзывается в день увольнения; общих логинов нет; роли пересматриваются раз в квартал

## 5. Рабочий лист по подрядчикам – строка на подрядчика

- [ ] Подрядчик _____ · медданные ✓/✗ · база в РФ ✓/✗ · поручение подписано ✓/✗
- [ ] Срок уведомления об инциденте ____ ч · медданные минимизированы ✓/✗ · владелец _____