Чек-лист: локализация и передача медданных

Прогоняйте при выборе стека, найме зарубежных подрядчиков и перед любой передачей данных пациентов за рубеж. Инженерные рекомендации, не юридическая консультация.

А. Карта хранилищ – локализация (ст. 18 ч. 5 152-ФЗ)

- [ ] Все базы с ПДн россиян – в РФ: основная, реплики, бэкапы, журналы, индексы, кэши
- [ ] CRM, хелпдеск, рассылки и облачные таблицы проверены на страну хранения
- [ ] Поручения подрядчикам требуют хранить и обрабатывать данные в РФ
- [ ] Автотест: новые хранилища и регионы облака – только российские

Б. Внешние зависимости – белый список

- [ ] Реестр потоков: сервис, страна, поручение, ПДн/медданные, уведомление, дата проверки
- [ ] Исходящий трафик контура данных – только к доменам из белого списка
- [ ] SDK мобильных сборок и CSP веб-приложения проверяются в CI
- [ ] Зарубежные аналитика, трекеры ошибок, CPaaS и ИИ-API не получают медданных
- [ ] Push-уведомления и письма без специальности, диагноза и времени приёма

В. Если передача за рубеж действительно нужна (ст. 12)

- [ ] Письменное согласие на спецкатегорию – отдельным документом, с получателем и страной
- [ ] Письменное согласие на раскрытие врачебной тайны (ст. 13 ч. 3 323-ФЗ)
- [ ] Сведения от получателя: меры защиты, условия прекращения обработки, реквизиты
- [ ] Уведомление РКН подано до начала; страна вне перечня – выждано 10 рабочих дней
- [ ] Минимальный набор; DICOM без лишних тегов; канал шифруется, передача журналируется
- [ ] Все передачи идут через один шлюз экспорта; копий шлюз не хранит

Г. Красные флаги – блокируют релиз

- [ ] Зарубежный SaaS используется как хранилище данных пациентов
- [ ] Иностранный подрядчик имеет доступ к продакшну с медданными
- [ ] Дампы продакшна в тестовых средах или у зарубежной команды
- [ ] «Уведомили РКН» используется как замена согласия пациента