Чек-лист: обезличивание и аналитика медданных

Прогоняйте перед подключением любого аналитического инструмента, пикселя, SDK или выгрузки данных. Инженерные рекомендации, не юридическая консультация.

А. Три выхода – каждый поток идёт ровно через один

- [ ] Выход 1, поручение: подрядчик в РФ, цель «анализ качества сервиса» названа в поручении
- [ ] Выход 2, согласие: письменное, отдельным документом, на конкретную цель (ст. 9, 10)
- [ ] Врачебная тайна для исследований и обучения ИИ – письменное согласие (ст. 13 ч. 3 323-ФЗ)
- [ ] Выход 3: наружу – только агрегаты; обезличенные записи остаются в сфере 152-ФЗ

Б. Аудит пейлоада – чего не должно быть за границей контура

- [ ] IP усекается или отбрасывается до сохранения; в выгрузках его нет
- [ ] URL и referrer без ID приёмов, специальностей врачей и названий клиник
- [ ] ID устройств, рекламные ID, телефоны, email, СНИЛС и полисы не покидают контур
- [ ] Хэши идентификаторов заменены случайными ключами; таблица ключей хранится отдельно
- [ ] Даты и возраст обобщены или сдвинуты; редкие комбинации подавлены (k-анонимность)
- [ ] Видео и аудио не выходят из контура; транскрипты – только после очистки и оценки риска

В. Двухзонный конвейер – проверки сборки

- [ ] Собственный эндпоинт сбора на вашем домене; сторонних скриптов в приложении нет
- [ ] Allowlist событий: новое событие или свойство – через pull request и ревью
- [ ] Хранилище событий и аналитика – в РФ; доступ по ролям, с журналом
- [ ] Агрегаты проходят подавление ячеек меньше k человек; k обосновано в модели угроз
- [ ] Обезличивание – воспроизводимая функция конвейера (готовность к требованию по 233-ФЗ)

Г. Красные флаги – блокируют релиз

- [ ] Пиксель или SDK внешнего сервиса в аутентифицированном приложении
- [ ] Сервер аналитики, краш-репортера или ИИ-API за рубежом
- [ ] «Мы обезличили» без ответа, где хранится дополнительная информация
- [ ] Вендор обезличивает данные после получения – передача уже произошла
- [ ] Push-уведомления или тикеты поддержки со специальностью врача или диагнозом