Ранбук наблюдаемости и эксплуатации телемедицины

Что наблюдать, на что настраивать алерты и как логировать без медданных. Инженерные рекомендации, а не юридическая консультация.

А. Доступность – это обязанность

- [ ] 152-ФЗ защищает ПДн и от блокирования и уничтожения (ст. 19 ч. 1), так что простой – это риск
- [ ] Резервные копии и восстановление: ОДТ приказа ФСТЭК № 21, ст. 19 ч. 2 п. 7, бэкапы ЭМД по 209н
- [ ] Сроки 193н (п. 19): экстренная консультация – от 30 мин до 2 ч, неотложная – от 3 до 24 ч

Б. Три слоя сигнала

- [ ] Слой 1 – инфраструктура: серверы, базы, сигналинг, API, доля ошибок. Нужно, но мало
- [ ] Слой 2 – видео каждой консультации: getStats() весь звонок – потери, джиттер, RTT, кадры
- [ ] Слой 3 – воронка: запись → вход (ЕСИА) → ожидание → соединение → завершено → протокол

В. SLO на уровне визита

- [ ] Соединение ≥ 99,5%; ожидание p95 < 10 с; обрывы < 1%; потери < 2% для ≥ 95% минут
- [ ] Бюджет ошибок: 99,9% ≈ 43 мин/мес, 99,99% ≈ 4,3. Исчерпан – спринт на надёжность; SLO ≠ SLA

Г. Алерты и дежурства

- [ ] Алерт – на симптом для пациента (соединения, обрывы, затор воронки), а не на загрузку CPU
- [ ] Покрытие 24/7: вечера, выходные, дистанционное наблюдение (193н п. 43–46), 11 часовых поясов
- [ ] Путь при кризисе (112, 103, телефоны доверия) – отдельный монитор высшей тяжести

Д. Логи без медданных, стек в России

- [ ] Два конвейера: журнал аудита (ст. 19 ч. 2 п. 8, РСБ) внутри границы; телеметрия очищена
- [ ] Только непрозрачные ID: без ФИО, телефонов, полисов и диагнозов в URL, ошибках, трейсах
- [ ] Self-hosted в российском облаке: Prometheus, Grafana, Loki, Sentry; зарубежный SaaS с ПДн – нет
- [ ] Подрядчик может увидеть медданные – поручение оператора (ст. 6 ч. 3). Зашифровано ≠ законно

Е. Выявление запускает отсчёт сроков

- [ ] Отсчёт – с момента выявления: вами, Роскомнадзором или посторонним исследователем
- [ ] Роскомнадзор: 24 ч – уведомление, 72 ч – итоги расследования (ст. 21 ч. 3.1 152-ФЗ)
- [ ] ГосСОПКА – 24 ч (приказ ФСБ № 77); значимый объект КИИ – НКЦКИ за 3 ч (приказ ФСБ № 547)