Чек-лист идентификации и доступа в телемедицине

Одна страница для проверки слоя идентификации: пациент, врач, справочник врачей и где лежат учётные записи. Инженерные рекомендации, не юридическая консультация – детали уточняйте у юриста.

1. Личность пациента

- [ ] Участники телемедконсультации идентифицируются через ЕСИА (ч. 6 ст. 36.2 323-ФЗ, п. 7 193н)
- [ ] Sber ID и VK ID – удобный вход для каталога, записи и оплаты; ЕСИА они не заменяют
- [ ] Сопоставление с картой в МИС – по устойчивому идентификатору (СНИЛС, полис ОМС), не по ФИО
- [ ] Распознавание по лицу – только через ЕБС или аккредитованную систему (572-ФЗ)

2. Вход и токены

- [ ] Второй фактор – минимум для любого доступа персонала к медданным; ключ – для админов
- [ ] В токенах (JWT) – только непрозрачные ID и scopes, никаких ФИО и диагнозов
- [ ] Повторное подтверждение перед доступом к записям и документам; частоту ЕСИА – с юристом

3. Вход врача и подпись

- [ ] SSO через IdP клиники по SAML 2.0 или OpenID Connect; брокер – Keycloak в российском контуре
- [ ] SCIM создаёт и отключает учётные записи: увольнение не должно ждать ручной заявки
- [ ] Протокол и ЭМД – с УКЭП медработника (ч. 7 ст. 36.2, 209н); подпись – не вход

4. Справочник врачей

- [ ] Врач в ФРМР, организация в ФРМО (п. 9 193н); то же – условие электронного рецепта (1094н)
- [ ] Лицензия покрывает дистанционные работы и услуги; аккредитация специалиста действующая
- [ ] Модель – FHIR Practitioner / PractitionerRole с кодами НСИ; сверка – регулярно
- [ ] Карточка врача для пациента (п. 37 193н) питается из того же справочника

5. Размещение и доступ

- [ ] Учётные записи с ПДн россиян – только в России (ст. 18 ч. 5 152-ФЗ); зарубежный IdP – не вариант
- [ ] Провайдер, хранящий учётные записи пациентов, работает по поручению обработки
- [ ] Аутентификация ≠ авторизация: роли, связь врач – пациент и журнал доступа к картам