Аутентификация и идентификация: чек-лист

Для продуктовой команды: ЕСИА, врачи и УКЭП, факторы, сессии и восстановление доступа. Инженерные рекомендации, а не юридическая консультация – детали уточняйте у юриста.

А. Личность пациента

- [ ] Разделены два контура: подтверждение личности (однажды) и аутентификация (каждый вход).
- [ ] Консультация – только после ЕСИА (ч. 6 ст. 36.2 323-ФЗ, п. 7 193н); Sber ID / VK ID её не заменяют.
- [ ] Нет вопросов-викторин (паспорт, адрес, девичья фамилия) – эти данные давно в утечках.
- [ ] Сопоставление с медкартой – по СНИЛС или полису ОМС; при сомнении – ручная проверка.
- [ ] Нет самодельной биометрии: распознавание лица – только через ЕБС или аккредитованную систему (572-ФЗ).

Б. Врач и персонал

- [ ] Врач – в ФРМР, организация – в ФРМО (п. 9 193н); лицензия и аккредитация сверены.
- [ ] Вход врача – через SSO клиники (SAML / OIDC) без отдельного пароля; второй фактор проверен.
- [ ] Учётная запись врача при онбординге связана с личностью, подтверждённой через ЕСИА.
- [ ] Протоколы, ЭМД и рецепты – с УКЭП (ч. 7 ст. 36.2, приказы 209н, 1094н); подпись – не вход.
- [ ] MFA для любого доступа персонала к медданным; FIDO2-ключи – для администраторов.

В. Факторы и сессии

- [ ] Основной фактор – passkey (FIDO2 / WebAuthn); SMS – только крайний запасной вариант.
- [ ] Блокировка сеанса по бездействию (УПД.10 приказа ФСТЭК № 21): время выбрано и записано.
- [ ] На общих станциях повторный вход – за секунды (passkey, токен), иначе таймаут обойдут.
- [ ] Step-up для рисковых действий: выгрузка медкарты, доступ вне расписания, смена реквизитов.

Г. Восстановление и сообщения

- [ ] Восстановление не слабее входа: врачи – через ИТ клиники, пациенты – через ЕСИА.
- [ ] Описан порядок при утрате и компрометации средств аутентификации (ИАФ.4 приказа № 21).
- [ ] В SMS, письмах и push нет специальности, врача и даты: тайна – уже сам факт обращения.
- [ ] Тест: «пациент потерял телефон – что требует восстановление и что раскрывает сообщение?»