Чек-лист готовности по 152-ФЗ и 323-ФЗ

Семь фаз по порядку, у каждого пункта – норма. Не юридическая консультация.

Фаза 1 · Роли и охват – ст. 18.1, 22.1 152-ФЗ

- [ ] Роль по каждому потоку данных записана; ответственный за обработку ПДн назначен приказом
- [ ] Инвентарь систем с медданными, карта потоков с границей контура; политика на сайте

Фаза 2 · Оценка – ст. 19 ч. 2 152-ФЗ, ПП 1119, приказ ФСТЭК № 21

- [ ] Модель угроз по инвентарю: тип угроз и уровень защищённости – с датой и подписью
- [ ] Оценка вреда пациентам; меры приказа № 21, компенсирующие – только с обоснованием

Фаза 3 · Документы и договоры – ст. 6, 9, 22 152-ФЗ; ст. 13 323-ФЗ

- [ ] Уведомление РКН подано до обработки; цели, меры, СКЗИ, место базы совпадают с реальностью
- [ ] Поручение по каждой стрелке к подрядчику; согласия отдельно; обязательства о неразглашении

Фаза 4 · Технические меры – ст. 19 152-ФЗ, приказ ФСТЭК № 21

- [ ] Уникальные учётки, второй фактор, ролевой доступ, журнал событий; базы и бэкапы в России
- [ ] Шифрование в канале и при хранении, СКЗИ – по модели угроз; оценка мер до запуска

Фаза 5 · Медицинский контур – ст. 36.2 323-ФЗ, 193н, ПП 852, ПП 140

- [ ] Лицензия покрывает услуги (п. 4); врачи в ФРМР, организация в ФРМО; ЕСИА и УКЭП
- [ ] Раскрытие по п. 37 193н; сопутствующие материалы – 1 год; ФЭР и РЭМД – 1 рабочий день

Фаза 6 · Люди и учения – ст. 18.1 ч. 1 п. 6, ст. 21 ч. 3.1 152-ФЗ

- [ ] Ознакомление под подпись; план реагирования 24/72 ч; журнал инцидентов и ложных тревог
- [ ] Тест восстановления с датой; ежегодный учебный запрос на 10 рабочих дней

Фаза 7 · Поддержание – ПП 1119, приказ № 21 п. 6, ст. 22 ч. 7 152-ФЗ

- [ ] Контроль и оценка мер – не реже раза в 3 года; модель угроз – при каждом изменении
- [ ] Уведомление РКН – до 15-го числа после изменений; проект замены № 21 – на контроле

Комплект доказательств – 14 вкладок для первого запроса

- [ ] 01 политика · 02 акты · 03 ознакомление · 04 контроль · 05 уведомление РКН · 06 модель угроз · 07 меры защиты · 08 поручения · 09 согласия · 10 инциденты · 11 лицензия · 12 п. 37 193н · 13 ЕСИА, УКЭП · 14 ЕГИСЗ