Шпаргалка по 152-ФЗ и врачебной тайне

Три слоя требований, тест роли, штрафы 2026 года и сроки при утечке на одной странице.

ТРИ СЛОЯ (152-ФЗ, 323-ФЗ)

Основания и врачебная тайна: кто видит медданные

Спецкатегория: по умолчанию запрет (ст. 10). Медицинские цели – у лиц, обязанных хранить врачебную тайну; прочее – письменное согласие отдельным документом. Минимум данных (ст. 5); ответ пациенту за 10 рабочих дней (ст. 20).

Безопасность: как защищать и где хранить

Модель угроз и уровень защищённости (ПП 1119). Меры приказа ФСТЭК № 21; СКЗИ ФСБ – где защита держится на криптографии. Базы с данными россиян – только в РФ (ст. 18 ч. 5).

Инциденты: если защита не сработала

Инцидент – неправомерная или случайная передача ПДн, нарушившая права. Отсчёт идёт с момента выявления, в том числе третьим лицом. Сведения направляются и в ГосСОПКА (ст. 19 ч. 12).

ШТРАФЫ ДЛЯ ЮРЛИЦ (ст. 13.11 КоАП)

ч. 1 – обработка с нарушением закона
150–300 тыс. ₽

ч. 10 – не уведомили о начале обработки
100–300 тыс. ₽

ч. 11 – не уведомили РКН об утечке
1–3 млн ₽

ч. 16 – утечка данных о здоровье
10–15 млн ₽

ч. 18 – повторная утечка спецкатегорий
1–3% выручки, от 25 до 500 млн ₽

ч. 8 и 9 – нарушение локализации
до 6 млн ₽; повторно до 18 млн ₽

Редакция 420-ФЗ, с 30.05.2025. Скидка 50% за быструю оплату не применяется. Уголовная ст. 272.1 УК РФ – с 11.12.2024. Нумерацию частей сверяйте с действующим текстом КоАП.

КТО ВЫ? (ст. 3 и 6 152-ФЗ)

Обработчик по поручению (большинство команд)

Обрабатываете данные по заданию клиники и в её целях. Нужно поручение: перечень данных и действий, цели, конфиденциальность, требования ст. 19, уведомление об инцидентах. Отвечаете перед оператором.

Оператор-медорганизация

Помощь оказывают ваши врачи по вашей лицензии. 152-ФЗ целиком + врачебная тайна + 193н: ЕСИА, ФРМР и ФРМО, уведомление РКН о начале обработки (ст. 22).

Самостоятельный оператор без лицензии

Каталог врачей, агрегатор, сервис психологов, велнес. Данные о здоровье – только по письменному согласию отдельным документом; врачебной тайны и телемедицины нет.

СРОКИ ПРИ УТЕЧКЕ: 24 И 72 ЧАСА

Пт 18:40 выявили → сб 18:40 РКН → пн 18:40 итоги

24 ч: факт, причины, вред, меры, контактное лицо. 72 ч: итоги расследования и виновные. Подача – через портал ПДн с входом через ЕСИА и электронной подписью.

Параллельные сроки

Значимый объект КИИ: НКЦКИ не позднее 3 ч (приказ ФСБ № 547). ГосСОПКА: при соглашении с НКЦКИ – туда за 24 ч, иначе через РКН. Не уведомили РКН – штраф 1–3 млн ₽. Подрядчик → оператор: срок в поручении – часы, а не дни.

ВОСЕМЬ ШАГОВ

- ☐ **Определите роль**
  оператор, обработчик по поручению или самостоятельный оператор
- ☐ **Карта медданных**
  системы, подрядчики, логи, бэкапы – и страна, где они лежат
- ☐ **Закрепите основания**
  поручение клиники или письменное согласие отдельным документом
- ☐ **Модель угроз и УЗ**
  ст. 19, ПП 1119; уровень – под целевой объём пациентов
- ☐ **Цепочка поручений**
  условия обработки на каждом узле; подрядчик за рубежом – нет медданных
- ☐ **Меры приказа № 21**
  шифрование, СКЗИ где нужно, второй фактор, роли, журнал, таймауты
- ☐ **Уведомления и план реагирования**
  ст. 22 для оператора; РКН за 24 и 72 часа; сроки подрядчиков
- ☐ **Документы и обучение**
  ст. 18.1, неразглашение врачебной тайны, оценка раз в 3 года

«Зашифровано» не значит «соответствует», «аттестовано» не значит «настроено», а значок «соответствует 152-ФЗ» юридической силы не имеет. Инженерные рекомендации, не юридическая консультация.

К статье «152-ФЗ и врачебная тайна простым языком для продуктовых команд»
fora-soft.ru/learn/telemedicine-video/articles-telemedicine/razrabotka-medprilozheniy-152-fz-i-vrachebnaya-tayna