**1. Как данные хранятся**

* **ФИО, контакты, дата рождения**:
  + Хранятся в зашифрованной базе данных (например, Postgres) с использованием AES-256.
  + Конфиденциальные данные разделены по доменам (PII, медицинские данные, финансовые данные), что минимизирует риск избыточного доступа.
* **Медицинские карты и результаты анализов**:
  + Хранятся в обезличенном виде, связаны с токенами, а не с реальными идентификаторами пациентов.
  + Оригинальные данные доступны только при строгой авторизации.
* **Финансовые данные**:
  + Хранятся в отдельной базе данных с дополнительным уровнем шифрования и изоляции.
  + Учет данных ведется в интеграции с «1С» через зашифрованные API.

**2. Периоды и условия уничтожения данных**

* **Периоды уничтожения**:
  + Данные пациентов хранятся в системе до 5 лет после завершения лечения в соответствии с законодательством РФ.
  + Лог-файлы доступа и операций удаляются через 1 год, если нет юридических причин их сохранения.
* **Условия уничтожения**:
  + По запросу клиента данные полностью удаляются из системы, включая резервные копии, в течение 30 дней.
  + Удаление осуществляется с помощью инструментов, поддерживающих безопасное стирание данных (например, алгоритмы DoD 5220.22-M).

**3. Способы защиты данных при хранении и передаче**

* **При хранении**:
  + Шифрование на уровне базы данных (Transparent Data Encryption).
  + Контейнеризация данных с использованием Role-Based Access Control (RBAC).
  + Маскирование данных в аналитических системах и отчётах.
* **При передаче**:
  + Используется TLS 1.3 для всех соединений.
  + Данные передаются через API, защищённые токенами OAuth 2.0.
  + Обезличивание данных перед передачей в лаборатории и партнёрские системы.

**4. Усиление Data Privacy**

* **Тегирование данных**:
  + Автоматическое добавление тегов PII, MEDICAL, FINANCIAL при создании записей в базе.
  + Использование этих тегов для ограничения доступа на уровне приложений.
* **Мониторинг и аудит**:
  + Внедрение системы SIEM для мониторинга доступа к данным.
  + Настройка алертов для выявления аномальной активности.
* **Разграничение доступа**:
  + Права доступа предоставляются строго в рамках роли (например, администратор, медицинский специалист, бухгалтер).
* **Резервное копирование**:
  + Резервные копии данных шифруются и хранятся отдельно от основной инфраструктуры.
  + Доступ к резервам возможен только после двухфакторной аутентификации.