Портал клиентов и сотрудников:

* Хранит минимальный набор персональных данных (email, телефон, ФИО), необходимый для идентификации пациента
* Ссылается на CRM систему по внутреннему идентификатору пациента, не хранит медицинские данные
* Использует HTTPS для передачи данных

CRM:

* Хранит персональные данные пациентов (ФИО, дата рождения, адрес, место работы, хронические заболевания и др.)
* Шифрует персональные данные перед сохранением в БД с использованием отдельного encryption key
* Предоставляет доступ на чтение данных только авторизованным сотрудникам согласно RBAC модели. Врачи имеют доступ только к своим пациентам.
* Логирует все обращения к конфиденциальным данным. Логи хранятся отдельно и доступны только безопасникам.
* По запросу пациента удаляет все его персональные данные из системы в течение 48 часов.

Платежный шлюз:

* Не хранит платежные данные пациентов, использует сторонний сервис процессинга платежей
* Сохраняет только обезличенную информацию о платежах для аналитики и отчетности

Интеграция с лабораторией:

* Передаёт только внутренний идентификатор пациента без персональных данных
* Шифрует все медицинские данные (назначения, результаты анализов) при передаче и хранении
* Автоматически удаляет данные анализов через 180 дней

Данны:

* Получает деперсонализированные обезличенные данные из систем (CRM, записи, платежи, анализы)
* Категоризирует данные по уровню конфиденциальности, шифрует при необходимости
* Предоставляет данные для BI, ML, AI только через защищённые API после валидации и очистки

Мониторинг и алертинг:

* Обрабатывает логи доступа к конфиденциальным данным из всех систем
* Выявляет аномальную активность и оповещает офицеров безопасности в реальном времени

Общие принципы:

* Разделение персональных и медицинских данных по разным доменам с контролем доступа
* Шифрование конфиденциальных данных при хранении и передаче
* Удаление неактуальных данных по истечении срока хранения
* Аудит доступа к конфиденциальным данным, выявление аномалий
* Возможность удаления всех данных пациента по запросу