CASE STUDY

HealthTech Company Builds Privacy Framework for Health Data at Scale

Company profile

- B2B HealthTech SaaS, Series A, ~60 employees
  - Processor / service provider to hospitals, processing patient health records
  - EU and UK markets, expanding into US
  - DPO driven by hospital procurement requirements and the nature and scale of health data processing

The problem

Two hospital procurement processes stalled. The company was processing special category health data across multiple EU member states with no formal privacy framework, no DPIAs, no health-data-specific policies, and no named DPO.

What we did (over 4 months)

- Health-data-specific privacy audit and DPIA, Article 9 legal basis analysis
  - DPO appointed, supervisory authority notified where required
  - Privacy policies rewritten for health data, patient rights, clinical workflows
  - Vendor DPA reviews, data retention framework (GDPR vs healthcare record-keeping)
  - Hospital procurement questionnaires completed
  - Staff training, breach response plan, US HIPAA gap assessment

Results

- Both hospital deals unblocked within 6 weeks
  - Health-data DPIA available for all future hospital customers
  - Reusable compliance package for hospital and clinic procurement
  - HIPAA gap assessment completed, foundation for US market entry