iOS App Store 上架要求研究報告

Apple App Store 審核指南重點

基本原則

- App Store 的指導原則：為用戶打造更安全可靠的 App 探索平台
- 每個 App 都會經過專家審核
- 編輯團隊每天幫助用戶發現新的 App
- 對每款 App 進行掃描，檢測惡意軟體和其他安全威脅

2024年最新技術要求

- 自2024年4月29日起，上傳到App Store Connect的App必須使用Xcode 15構建
- 必須針對iOS 17、iPadOS 17、Apple tvOS 17或watchOS 10構建

五大審核分類

1. **安全 (Safety)**
2. 不得包含令人反感、攻擊性或低俗內容
3. 用戶生成內容需要適當的過濾機制
4. 兒童安全保護措施
5. **性能 (Performance)**
6. App不得發生崩潰或存在錯誤
7. 所有功能必須正常運作
8. 需要提供完整的測試環境
9. **商務 (Business)**

10. 清楚的商業模式
11. 合規的付費機制
12. 透明的訂閱和內購項目
13. **設計 (Design)**
14. 符合Apple設計指南
15. 良好的用戶體驗
16. 適當的介面設計
17. **法律 (Legal)**
18. 遵守當地法律法規
19. 隱私政策合規
20. 知識產權保護

提交前檢查清單

- 測試App是否會發生崩溃、是否存在錯誤
- 確保所有App信息及元數據完整且正確
- 更新聯繫信息
- 提供App的完整訪問權限
- 如有基於帳戶的功能，提供有效的演示帳戶
- 啟用後台服務
- 在App審核備註中附上詳細說明

特殊注意事項

- 兒童保護：很多兒童會大量下載App，需要特別注意內容適宜性
- 全球分發：App Store面向全球數億用戶
- 內容審查：所有觀點都受支持，但必須尊重用戶並提供良好體驗
- 反欺詐：嚴禁欺騙系統、竊取用戶數據、抄襲作品等行為

醫療健康類App特殊要求

（需要進一步研究具體醫療類App的特殊規定）

醫療健康類App特殊要求

基礎概念區分

適用範圍

- **FDA**：適用於涉及"醫療功能"的App（如疾病診斷、治療建議、用藥提醒等）
- **HIPAA**：適用於處理美國境內"受保護健康信息（PHI）"的實體（如醫院、保險機構及合作方）
- **GDPR**：適用於處理歐盟用戶個人數據（含健康數據）的所有App，無論公司所在地

關鍵判斷標準

- 若App僅記錄步數/心率（無醫學建議），可能不涉及FDA/HIPAA
- 若App存儲用戶病歷或對接醫療機構，則需同時考慮HIPAA和GDPR

FDA合規要點（醫療功能類App）

是否需要註冊?

- **Class I低風險**（如健康追蹤）：通常豁免（但需自我認證）
- **Class II/III高風險**（如血糖監測、AI診斷）：需FDA審批（510(k)或PMA流程）
- 示例：Apple Watch ECG功能已通過FDA Class II認證

必須行動

- 明確App功能是否屬於"醫療設備"（參考FDA《Mobile Medical Applications Guidance》）
- 若需審批，需與法律顧問合作提交材料（周期可能長達12個月+）

風險規避

- 避免宣稱治療/診斷疾病（除非通過審批）
- 用戶界面需標註"非醫療建議"（如健身類App）

HIPAA合規要點（涉及美國醫療數據）

誰必須遵守?

- **Covered Entities**：醫院、診所、保險公司
- **Business Associates**：為其處理PHI的第三方（如雲服務商、數據分析公司）

核心要求

- **數據加密**：傳輸（TLS 1.2+）和存儲（AES-256）加密
- **訪問控制**：角色權限管理（如醫生vs患者）
- **用戶權利**：允許用戶查看/刪除/導出數據（響應時限30天內）
- **BA協議**：與第三方簽署《Business Associate Agreement》（BAA）

GDPR合規要點（涉及歐盟用戶）

健康數據屬於"特殊類別數據"，需額外保護：

- 必須獲得用戶**明確同意**（非默認勾選，需提供撤回選項）
- 實現**數據最小化**（僅收集必要數據）

關鍵權利保障

- **數據可攜權**：允許用戶導出數據（如CSV/JSON格式）
- **被遺忘權**：收到刪除請求後72小時內執行
- **DPIA評估**：高風險數據處理前需做《數據保護影響評估》

iOS平台特殊要求

App Store審核

- 若涉及健康數據，需在隱私政策中明確用途

- 使用Apple HealthKit時需：
- 禁止將數據用於廣告/第三方共享（除非用戶授權）
- 提供獨立的健康數據使用條款

技術實現建議

- 本地存儲優先（減少服務器端PHI存儲）
- 使用iOS原生加密API（如Keychain Services）

合規實施檢查清單

步驟	行動項
1	確認App是否屬於FDA監管範圍（諮詢法律顧問）
2	若處理美國醫療數據：簽署BAA、加密PHI
3	若涉及歐盟用戶：更新隱私政策、部署同意管理平台（CMP）
4	在App內提供：數據訪問/刪除入口、合規聲明
5	每年進行第三方合規審計（重點檢查數據日誌）

常見錯誤案例

- **錯誤**：未加密存儲用戶病歷 → HIPAA罰款$250,000
- **錯誤**：將德國用戶健康數據傳至美國服務器 → GDPR罰款4%年營收
- **錯誤**：宣稱"AI可替代醫生診斷" → FDA強制下架