# Product Requirements Document (PRD) — 線上醫院掛號與診務系統

版本：0.2 作者：Product Manager 參考文件：project-brief.md, prd-and-planning-draft.md

目錄

# 醫療管理系統需求文件

## 1.0 模組：使用者與身分管理

涵蓋系統所有角色（病患、醫生、管理員）的帳號註冊、身份驗證、個人資料管理、以及系統級的帳號與權限管理功能。

| 功能編號 | 功能名稱 | 功能說明 |
| --- | --- | --- |
| 1.1 | 病患註冊 | 病患可註冊或由管理員建立帳號。 |
| 1.2 | 帳號建立 | 管理員建立所有帳號與角色權限 |
| 1.3 | 帳號修改 | 管理員修改所有帳號與角色權限 |
| 1.4 | 帳號刪除 | 管理員刪除所有帳號與角色權限 |
| 1.5 | 使用者登入 | 所有使用者（病患、醫生、管理員）可登入系統。 |
| 1.6 | 使用者登出 | 所有使用者（病患、醫生、管理員）可登出系統。 |
| 1.7 | 修改個人資料 | 所有使用者可修改自己的基本資料 |

## 2.0 模組：門診與班表管理

提供門診班表的完整管理功能，管理員可以新增、修改、刪除醫生的門診時段，病患可以查詢門診班表。

| 功能編號 | 功能名稱 | 功能說明 |
| --- | --- | --- |
| 2.1 | 管理員新增醫生班表 | 管理員可以為醫生新增門診時段 |
| 2.2 | 管理員修改醫生班表 | 管理員可以修改已建立的門診時段資訊 |
| 2.3 | 管理員刪除醫生班表 | 管理員可以刪除不再需要的門診時段 |
| 2.4 | 醫生停診管理 | 醫生申請停診，管理員審核並自動通知受影響病患 |
| 2.5 | 醫生查看個人班表 | 醫生可以查詢自己的門診排班表 |
| 2.6 | 查詢醫生班表 | 病患、管理員可以根據權限，依科別或醫生姓名查詢各類門診班表，查看可預約的日期與時段及剩餘掛號名額 |

## 3.0 模組：線上掛號

提供病患完整的線上掛號功能，病患可以新增、修改、取消掛號，並查詢掛號結果。

| 功能編號 | 功能名稱 | 功能說明 |
| --- | --- | --- |
| 3.1 | 病患新增掛號 | 病患可以選擇科別、醫生、日期與時段進行線上掛號 |
| 3.2 | 病患修改掛號 | 病患可以在截止時間前修改已預約的掛號時段 |
| 3.3 | 病患刪除掛號 | 病患可在截止時間前取消已預約的掛號，系統會釋放該時段名額 |
| 3.4 | 病患查詢掛號結果 | 病患可以查詢自己的掛號記錄，包括歷史掛號與未來預約，查看掛號狀態與詳細資訊 |

## 4.0 模組：報到

提供病患到院後的報到功能，支援線上報到與現場報到，並提供即時候診資訊與補號機制。

| 功能編號 | 功能名稱 | 功能說明 |
| --- | --- | --- |
| 4.1 | 病患線上報到 | 病患可以線上報到，系統會將病患加入候診佇列 |
| 4.2 | 病患現場報到 | 病患可以現場使用機台報到，包含處理過號問題 |
| 4.3 | 過號/爽約懲罰 | 累積過號/爽約達門檻後，系統自動限制病患只能現場報到 |
| 4.4 | 即時看診資訊 | 病患報到後可以即時查看當前看診號碼、自己的候診順序、前方等候人數及預估等候時間 |

## 5.0 模組：病歷

提供完整的病歷管理功能，醫生可以新增、修改病歷記錄，病患可以查詢自己的歷史病歷資料。

| 功能編號 | 功能名稱 | 功能說明 |
| --- | --- | --- |
| 5.1 | 歷史病歷查詢 | 病患及醫生可以根據權限，查詢相關的歷史就診記錄，包括診斷內容、處方用藥、檢查報告等詳細資訊 |
| 5.2 | 醫生新增病歷 | 醫生在看診後可以建立病歷記錄 |
| 5.3 | 醫生修改病歷 | 醫生可以修改病歷內容，補充或更正診斷與處方資訊。 |
| 5.4 | 醫生刪除病歷 | 醫生可刪除錯誤建立的病歷記錄 |
| 5.5 | 審計日誌檢視 | 系統管理員搜尋/匯出所有病歷操作的審計日誌 |
| 5.6 | 存取控管（RBAC） | 系統支援基於角色的存取控管，細分讀寫權限 |

## 6.0 模組：診務通知與管理儀表板

提供自動化的通知服務，系統會在關鍵時點自動發送通知給病患，確保病患不會錯過就診時間。

| 功能編號 | 功能名稱 | 功能說明 |
| --- | --- | --- |
| 6.1 | 掛號結果通知 | 病患完成掛號後，系統會立即發送確認通知（Email），包含掛號序號、醫生姓名、看診時間及診間位置 |
| 6.2 | 門診流量儀表板 | 管理員查看即時門診流量、診間負載與 KPI 報表 |
| 6.3 | 看診提醒通知 | 系統會在看診前一天自動發送提醒通知給病患，提醒就診時間與注意事項 |

## 系統角色說明

* **病患（Patient）**：可進行註冊、掛號、報到、查詢病歷等操作
* **醫生（Doctor）**：可管理個人班表、處理病歷、申請停診等操作
* **管理員（Administrator）**：可管理所有帳號、班表、查看系統報表等操作 +======================+======================================================================================+================+=============================================================================================+

## 2. 範圍摘要（MVP 範圍）

* 含：六大核心模組（同上）
* 排除：急診特殊流程、遠距醫療/視訊診療、第三方線上付費/保險整合

## 3. 系統分析（圖表 — Mermaid 語法）

### 3.1 Use Case Diagram

%% Use Case Diagram for Online Hospital Registration System  
actor Patient as 病患  
actor Doctor as 醫師  
actor Admin as 管理員  
  
rectangle System {  
 病患 -- (註冊/登入)  
 病患 -- (查詢班表)  
 病患 -- (線上掛號/預約)  
 病患 -- (線上報到/Kiosk報到)  
 病患 -- (查看病歷摘要)  
 痑  
 醫師 -- (登入)  
 醫師 -- (查看班表)  
 醫師 -- (停診申請)  
 醫師 -- (編輯病歷)  
 管理員 -- (管理班表)  
 管理員 -- (管理帳號)  
 管理員 -- (查看儀表板)  
}

短述：此 Use Case 圖展示三種主要使用者（病患、醫師、管理員）與系統間的互動，涵蓋註冊、查詢班表、掛號、報到、病歷存取與管理後台功能。

### 3.2 Swimlane Diagram（病患線上掛號到到診報到的完整流程）

```mermaid

%% Swimlane for patient booking to check-in

%% lanes: Patient, System, ClinicStaff

sequenceDiagram

    participant P as 病患

    participant S as 系統

    participant C as 醫護/管理

    P->>S: 查詢班表/選擇時段

    S-->>P: 顯示可用時段

    P->>S: 提交預約

    S-->>P: 回傳預約編號 + 提醒設定

    P->>S: 線上報到（到院前）

    S-->>C: 通知病患已報到

    C-->>S: 更新候診狀態

    S-->>P: 發送號碼接近提醒

    P->>C: 到診並進入診間

```

短述：此泳道（Swimlane）序列圖描述病患從班表查詢、預約、線上報到到收到就診提醒的端到端流程，並標示系統與醫護端之間的通訊點。

### 3.3 ERD（核心實體關係圖）

```mermaid

erDiagram

    PATIENT {

        string patient\_id PK

        string name

        date dob

        string phone

        string email

    }

    DOCTOR {

        string doctor\_id PK

        string name

        string specialty

    }

    APPOINTMENT {

        string appointment\_id PK

        string patient\_id FK

        string doctor\_id FK

        datetime start\_time

        datetime end\_time

        string status

    }

    SCHEDULE {

        string schedule\_id PK

        string doctor\_id FK

        date date

        time start

        time end

    }

    MEDICAL\_RECORD {

        string record\_id PK

        string patient\_id FK

        string doctor\_id FK

        datetime created\_at

        text summary

    }

    AUDIT\_LOG {

        string log\_id PK

        string user\_id

        string action

        datetime timestamp

        string target\_id

    }

    PATIENT ||--o{ APPOINTMENT : books

    DOCTOR ||--o{ APPOINTMENT : receives

    DOCTOR ||--o{ SCHEDULE : has

    PATIENT ||--o{ MEDICAL\_RECORD : has

    DOCTOR ||--o{ MEDICAL\_RECORD : authors

    AUDIT\_LOG ||--o{ MEDICAL\_RECORD : logs

```

短述：ERD 定義了病患、醫師、班表、預約、病歷與審計日誌的主要實體與關聯，用以支援預約與病歷操作的資料模型基礎。

## 4. Epics 與 User Stories（完整整合）

以下為整合後的所有 Epics 與 User Stories，包含完整的驗收標準（Acceptance Criteria）。

#### Epic A — 使用者與身分管理（User Management）

描述：建立統一的身份驗證與授權服務，支援病患、醫師、管理員角色與權限管理。

User Story A1 - 描述：作為一名病患，我希望能在線上註冊帳號並填寫聯絡資訊，以便完成預約與接收通知。 - 驗收標準： - 病患可以使用電子郵件或手機號碼註冊帳號並完成電子郵件/手機驗證。 - 註冊流程包含必填欄位：姓名、生日、聯絡電話、電子郵件、健保卡號（可用模擬值）。 - 註冊完成後自動建立病患檔案並能即時用於預約流程（新建立的帳號在 5 分鐘內能呼叫預約 API）。

User Story A2 - 描述：作為一名醫師，我希望能使用醫院提供的帳號登入系統，以便查看個人班表與病患報到狀態。 - 驗收標準： - 醫師可透過 SSO（若醫院提供）或系統帳號登入，登入成功率 >= 99%（非網路中斷情況）。 - 登入後 3 秒內顯示今日班表與當下候診名單（在測試資料環境）。

User Story A3 - 描述：作為管理員，我希望能建立與管理不同角色帳號，以控管系統存取權限。 - 驗收標準： - 管理員可新增/停用/修改帳號角色（病患/醫師/管理員）。 - 該操作需被記錄到審計日誌，包含操作者 ID、時間戳與變更摘要。

User Story A4 (安全) - 描述：作為系統管理者，我希望系統支援密碼重設與多因素驗證（可選），以提高帳號安全。 - 驗收標準： - 使用者可發起密碼重設流程並透過驗證碼完成重設。 - 系統可啟用 OTP 類型的多因素驗證；啟用後登入需額外通過 MFA。

#### Epic B — 門診與班表管理（Clinic & Schedule Management）

描述：提供班表 CRUD、班表查詢，以及醫師停診申請與管理員核准流程。

User Story B1 - 描述：作為病患，我要能查詢某科別或特定醫師的班表，以方便選擇時段預約。 - 驗收標準： - 病患可依科別、醫師名稱或日期篩選班表。 - 查詢結果在 2 秒內返回（在正常負載下）。

User Story B2 - 描述：作為醫師，我要能提交『停診申請』並附上停診原因，以便管理員處理並自動通知受影響病患。 - 驗收標準： - 醫師可為未來日期提出停診申請，需包含停診時段、原因與備註。 - 管理員在介面能看到待審核的停診申請並能核准或拒絕，核准後系統自動更新班表並發送通知給受影響的預約者。

User Story B3 - 描述：作為管理員，我希望能快速新增或調整臨時班次以應對流量變化。 - 驗收標準： - 管理員在 5 分鐘內能新增臨時班次並同步至病患查詢介面。 - 新增/修改班次的操作會被記錄於審計日誌。

#### Epic C — 線上掛號與預約（Registration & Scheduling）

描述：病患線上查看時段、掛號、候補與提醒流程；不含先付款。

User Story C1 - 描述：作為病患，我希望能在行動裝置上選擇科別、醫師和時段完成掛號。 - 驗收標準： - 病患可選擇科別/醫師/時段並提交預約申請，系統回傳預約編號。 - 若時段已滿，病患可加入候補清單並收到候補成功通知。

User Story C2 - 描述：作為病患，我希望在預約前收到可視化的時段可用性（即時），以做出選擇。 - 驗收標準： - 顯示的時段可用性為系統實際狀態（在 5 秒內更新）。 - 系統在建立預約時對時段做最終鎖定，避免雙重預約。

User Story C3 - 描述：作為管理員，我希望設定自動提醒規則（例如提前 48h、24h、2h），以降低爽約率。 - 驗收標準： - 可配置的提醒模板可選擇透過 SMS/Email/推播發送，模板支援簡短與詳細兩種格式。 - 系統紀錄每次提醒發送結果（送達/失敗）。

#### Epic D — 到診報到與候診排隊（Check-in & Queue Management）

描述：支援線上報到、Kiosk 報到、實時排隊與過號處理（簡化急診情境）。

User Story D1 - 描述：作為病患，我希望能在線上或 Kiosk 完成報到，避免現場排長龍。 - 驗收標準： - 病患可於預約時段前線上報到，系統在報到後更新候診名單並通知對應診間。 - 報到流程在 30 秒以內完成（含網路延遲）。

User Story D2 - 描述：作為病患，我希望在號碼即將到達時收到提醒，以便提早準備進診間。 - 驗收標準： - 系統於號碼前兩名時發送單向提醒給病患（SMS/推播），並記錄發送結果。

User Story D3 - 描述：作為管理員，我希望系統能自動處理過號情況（例如重新候補或自動取消並通知病患），以維持候診秩序。 - 驗收標準： - 系統能依預設規則判定過號並執行指定動作（重新候補或取消），並發送通知。 - 任何過號導致的狀態變更都有審計紀錄。

User Story D4 (過號/爽約懲罰) - 描述：作為系統，我需要監控並記錄病患的過號/爽約次數，當某病患在 90 天內累積 >= 3 次過號/爽約後，自動限制其只能改為現場 Kiosk 報到（禁止線上報到），以提升整體遵從率。

驗收標準： - 系統能記錄每次預約的狀態（完成／到診／過號／爽約），並能在病患層級計算過號／爽約次數（可設定時間窗口，預設 90 天）。 - 當病患在設定窗口內累計過號／爽約達到門檻（預設 3 次）時，系統會自動： 1. 將該病患的帳號標記為「限制線上報到」狀態（此狀態使 UC-QM-01 無效）。 2. 在病患嘗試使用線上報到（UC-QM-01）時阻止其完成報到，並顯示明確訊息提示其轉往現場機台（包含剩餘限制天數與申訴流程連結）。 3. 自動發送通知（Email/SMS/推播）告知病患被限制線上報到及解鎖條件（通知結果需記錄）。 - 系統提供管理員介面檢視被限制之病患名單，並支援手動解除限制（手動操作需寫入審計日誌）。 - 新增（門診結束結算）驗收標準：系統在門診時間結束時會檢查所有已被標記為「過號觀察期」但尚未執行 UC-QM-02（現場機台報到）的病患，將其最終狀態標記為「爽約 (No-Show)」，並將該次計入懲罰次數／累計，觸發上述限制邏輯（若因此達到門檻）。

#### Epic E — 病歷資料管理（Electronic Health Record Management）

描述：提供病歷的查詢與（受控的）醫師編輯能力，強調資料完整性、審計日誌與嚴格的存取權限控制。

User Story E1 - 描述：作為病患，我希望能查看並下載我的就診摘要與檢驗報告，以便自主管理健康紀錄。 - 驗收標準： - 病患可在個人介面查看最近 N 次就診摘要與檢驗報告（N 由醫院設定，預設 12 個月）。 - 病患可下載 PDF 格式的就診摘要，但無法修改病歷內容。

User Story E2 - 描述：作為醫師，我希望能新增診療筆記與上傳檢驗報告，以記錄臨床決策並供後續查詢。 - 驗收標準： - 醫師可新增或修改診療筆記，所有變更需包含操作者 ID 與時間戳，並被寫入不可變更的審計日誌中。 - 上傳檔案需通過病毒掃描與格式檢查，成功上傳後能在病患查詢介面顯示連結（依存取權限）。

User Story E3 - 描述：作為系統管理員，我希望有可搜尋的審計日誌，能回溯誰在何時對哪筆病歷做了什麼操作，以配合法務或稽核需求。 - 驗收標準： - 審計日誌包含：操作者 ID、操作類型（新增/修改/刪除/檢視）、目標病歷 ID、時間戳、來源 IP/裝置識別（若可得）。 - 日誌不可被系統使用者刪除，並支援匯出（CSV/JSON）以便法務或稽核使用。

User Story E4 (存取控管) - 描述：作為資安負責人，我希望系統能支援基於角色的存取控管（RBAC）並細分敏感欄位的讀寫權限，以符合法規。 - 驗收標準： - 系統支援角色與權限矩陣：醫師可讀寫其負責病患之完整病歷；行政僅能讀取非敏感欄位（如聯絡資訊）；病患僅能讀取摘要。 - 任一嘗試未授權存取的行為會被阻擋並寫入審計日誌，且管理員可在 1 小時內收到異常警示（若設定）。

#### Epic F — 診務通訊與管理儀表板（Communication & Admin Dashboard）

描述：實作院內單向通知機制與運營儀表板，用以支援醫護與管理決策。

User Story F1 - 描述：作為管理員，我希望在儀表板上看到即時門診流量與各診間負載，以便快速調配人力。 - 驗收標準： - 儀表板在 5 秒內更新當前候診人數與診間負載（在正常資料流下）。

User Story F2 - 描述：作為醫護人員，我希望在病患到診或取消時收到系統通知，以便調整門診安排。 - 驗收標準： - 病患報到或取消事件會在 30 秒內觸發內部通知至相關醫護端，並記錄送達結果。

User Story F3 - 描述：作為病患，我希望在我的看診號碼接近時收到單向提醒，以便準備就診。 - 驗收標準： - 在號碼前兩名時發送單向提醒到病患，並記錄送達狀態；若送達失敗，系統保留重新嘗試策略或告知管理員手動處理。

## 5. Use Case 詳細文字敘述與 Activity Diagram

### Use Case：病患新增掛號（Patient Creates Appointment）

* 主要參與者：病患、系統、醫院資料介面
* 前置條件：病患已註冊並登入，醫師班表已上傳至系統
* 主要流程：
  1. 病患登入系統並進入「掛號」頁面。
  2. 病患選擇欲看診的科別與醫師，系統顯示該醫師的可用時段。
  3. 病患選擇時段並填寫必要就診資訊（如主訴），提交預約請求。
  4. 系統檢查時段可用性並鎖定時段，建立預約記錄，回傳預約編號。
  5. 系統依預設提醒策略排程提醒（48h、24h、2h）並在必要時發送確認通知。
  6. 若時段已滿或衝突，系統提示病患加入候補清單。
  7. 流程完成。

#### Activity Diagram（Mermaid）

```mermaid

flowchart TD

  A[病患登入] --> B[查看班表]

  B --> C{時段可用?}

  C -- 是 --> D[填寫預約資訊]

  D --> E[系統鎖定時段並建立預約]

  E --> F[回傳預約編號]

  E --> G[排程提醒]

  C -- 否 --> H[加入候補]

  H --> F

```

### Use Case：醫師停診申請（Doctor Requests Leave）

* 主要參與者：醫師、系統、管理員、病患（可能受影響）
* 前置條件：醫師已登入系統並查看個人班表
* 主要流程：
  1. 醫師於系統中選擇欲停診的日期/時段並填寫停診原因。
  2. 系統建立停診申請並將申請狀態設為「待審核」。
  3. 管理員在後台接收申請，審核後核准或拒絕。
  4. 若核准，系統自動更新班表，將受影響的預約標記為需重排，並通知受影響之病患（Email/SMS）。
  5. 流程完成。

#### Activity Diagram（Mermaid）

```mermaid

flowchart TD

  A[醫師登入] --> B[提出停診申請]

  B --> C[系統建立申請 - 待審核]

  C --> D[管理員審核]

  D -- 核准 --> E[系統更新班表]

  E --> F[通知受影響病患]

  D -- 拒絕 --> G[通知醫師]

```

## 6. 非功能性需求（NFRs）

1. 效能（Performance）

  - 目標：系統在平常時段所有核心查詢（班表查詢、預約查詢、候診人數）應於 95th 百分位小於 1.5 秒回應（在測試資料與預期負載下）。

  - 高峰期（例如早上 08:00–09:30）仍需保證列表/查詢型 API 95th 百分位 < 2.5 秒；預約建立 API 的 95th 百分位 < 3 秒（含鎖定邏輯）。

2. 安全與合規（Security & Compliance）

  - 傳輸層：所有 API 與前端通訊使用 TLS 1.2+（建議 TLS 1.3）。

  - 靜態資料保護：所有敏感資料（病歷內容、身份識別資訊）在儲存時至少使用 AES-256 加密。

  - 存取控管：實作 RBAC，支援最小權限原則，並支援 SSO（若醫院提供）與 MFA 作為選項。

  - 審計日誌：所有病歷讀/寫/刪操作需寫入不可變更的審計日誌（包括操作者、時間戳、來源），日誌需保存至少 7 年或依醫院合規要求。

  - 資安測試：上線前需完成靜態程式碼掃描、動態弱點掃描（DAST）與一次穿透測試（可由第三方執行）。

3. 可用性（Availability / SLA）

  - 目標：系統可用性 SLA 初步設定為 99.9%（每年可接受停機時間約 8.77 小時）。

  - 關鍵元件（身份驗證、預約建立、通知管線）需具備基本重試機制與降級模式（例如通知失敗時記錄並重試）。

4. 可維運性（Maintainability）

  - 系統需提供監控與告警（CPU、記憶體、API 延遲、錯誤率、通知失敗率），並能匯出使用與錯誤日誌以協助排查。

5. 可擴展性（Scalability）

  - 設計 API 與資料層以支援橫向擴充（stateless API、Redis/隊列協助排隊計數）。

## 7. Use Case 規格（逐一詳述）

下列為你指定的 14 個 Use Case 的完整規格，每個 Use Case 包含：主要動作者、商業流程編號、摘要、前置/後置條件、主要流程與替代/異常流程，並附上 Mermaid 活動圖以利視覺化。

### UC-SC-04 醫師停診申請 / 管理員審核 (Doctor Leave Request / Admin Review)

* 主要動作者 (Primary Actor)：醫師（Doctor）、管理員（Administrator）
* 商業流程編號 (Business Process ID)：BP-SC-04
* 摘要描述：醫師於系統提出停診申請，管理員審核後核准或拒絕；若核准，系統更新班表並通知受影響病患與相關單位。
* 前置條件：醫師已登入且為該醫師帳號；申請日期位於未來且可被編輯。
* 後置條件：停診申請記錄狀態為「核准／拒絕／待審核」，受影響預約被標記為需重排（若核准），通知發出且審計日誌記錄該操作。
* 主要流程：
  1. 醫師選擇日期/時段並在系統填寫停診原因與備註，送出申請。
  2. 系統建立停診申請（狀態：待審核）並通知管理員有新申請。
  3. 管理員在審核介面檢視申請內容、檢視受影響預約清單，並選擇核准或拒絕。
  4. 若管理員核准：系統將班表更新為停診、將受影響預約標記為需重排並自動發送通知給受影響病患（Email/SMS），並寫入審計日誌；若拒絕：系統通知申請醫師並寫入審計日誌。
* 替代/異常流程：
  + A1：若管理員在審核期間發現衝突需額外確認，則將申請標記為「需更多資訊」並要求醫師補件；流程暫停直到補件完成。
  + A2：若自動通知發送失敗，系統依重試策略重試並在管理儀表板上標示失敗紀錄以供人工處理。

flowchart TD  
 A("醫師提出停診申請") --> B("系統建立申請 (待審核)")  
 B --> C("通知管理員")  
 C --> D("管理員審核")  
 D -- "核准" --> E("系統更新班表")  
 E --> F("標記受影響預約為需重排")  
 F --> G("發送通知給病患")  
 D -- "拒絕" --> H("通知醫師並寫入審計")  
 G --> I("寫入審計日誌")  
 I --> EndNode(("結束"))

### UC-RS-01 病患新增掛號（Patient Creates Appointment）

* 主要動作者：病患（Patient）
* 商業流程編號：BP-RS-01
* 摘要描述：病患於前端選擇科別/醫師/時段進行線上掛號；系統鎖定時段並回傳預約編號。
* 前置條件：病患已註冊並登入；欲預約之醫師班表已公開且有可用時段。
* 後置條件：建立預約記錄（status: confirmed 或 waitlist），系統建立提醒並寫入審計。
* 主要流程：
  1. 病患選擇科別與醫師並查詢可用時段。
  2. 系統顯示即時可用性並鎖定所選時段（短時間交易鎖定）。
  3. 病患填寫必要資料並提交。
  4. 系統建立預約（若有名額則 confirmed；否則加入候補），回傳預約編號並建立提醒。
* 替代/異常流程：
  + A1（鎖定失敗）：若鎖定時段失敗，回覆錯誤並提示重新查詢/重試。
  + A2（候補）：若時段已滿，病患可選擇加入候補，系統通知候補結果。

flowchart TD  
 Start([開始]) --> Search("查詢班表")  
 Search --> Lock("系統鎖定時段")  
 Lock -- "成功" --> Submit("病患提交預約")  
 Lock -- "失敗" --> Fail("提示鎖定失敗")  
 Submit --> Create("建立預約紀錄")  
 Create -- "有名額" --> Confirm("回傳預約編號 (confirmed)")  
 Create -- "無名額" --> Waitlist("加入候補並回傳候補編號")  
 Confirm --> EndNode2(("結束"))  
 Waitlist --> EndNode2  
 Fail --> EndNode2

### UC-RS-02 病患修改掛號（Patient Modifies Appointment）

* 主要動作者：病患（Patient）
* 商業流程編號：BP-RS-02
* 摘要描述：病患在截止時間內修改已預約之時段；系統重新鎖定並更新預約。
* 前置條件：病患為原預約擁有者並已登入；尚未超過修改截止時間；預約狀態允許修改。
* 後置條件：預約更新成功，舊時段釋放，新時段鎖定並寫入審計。
* 主要流程：
  1. 病患於個人預約頁面選擇欲修改之預約並啟動修改。
  2. 病患選擇新時段、系統嘗試鎖定新時段。
  3. 系統若鎖定成功則更新預約並釋放原時段，通知病患與相關診間；若鎖定失敗則提示錯誤。
* 替代/異常流程：
  + A1（超過截止）：若超過修改截止時間，系統拒絕線上修改並提示聯絡客服或至現場辦理。
  + A2（衝突）：若新時段在鎖定過程中被他人搶先預約，系統提示並提供候補或其他時段選項。

flowchart TD  
 Start --> Select[選擇欲修改之預約]  
 Select --> ChooseNew[選擇新時段]  
 ChooseNew --> LockNew[嘗試鎖定新時段]  
 LockNew -->|成功| Update[更新預約並釋放舊時段]  
 LockNew -->|失敗| Conflict[提示時段衝突]  
 Update --> Notify[通知病患與診間]  
 Notify --> End  
 Conflict --> End

### UC-RS-03 病患取消掛號（Patient Cancels Appointment）

* 主要動作者：病患（Patient）
* 商業流程編號：BP-RS-03
* 摘要描述：病患於取消截止時間前可線上取消預約；系統釋放名額並處理候補遞補。
* 前置條件：病患為預約擁有者並已登入；預約狀態允許取消且在取消期限內。
* 後置條件：預約標記為已取消，釋放名額，若候補存在則遞補並通知候補者；審計日誌更新。
* 主要流程：
  1. 病患選擇取消預約並確認。
  2. 系統將預約狀態設為已取消並釋放名額。
  3. 系統檢查候補清單並依序遞補（若有候補），通知新取得名額之病患。
* 替代/異常流程：
  + A1（超過取消期限）：若超過取消截止時間，系統禁止線上取消並提示至櫃檯或客服。
  + A2（通知失敗）：若遞補通知失敗，系統記錄失敗並依重試策略處理或提示管理員。

flowchart TD  
 Start --> SelectCancel[病患選擇取消]  
 SelectCancel --> Confirm[系統確認並標記取消]  
 Confirm --> Release[釋放名額]  
 Release --> CheckWaitlist[檢查候補]  
 CheckWaitlist --> |有候補| Promote[遞補並通知候補者]  
 CheckWaitlist --> |無候補| End  
 Promote --> End

### UC-RS-04 病患查詢掛號結果（Patient Views Appointment Records）

* 主要動作者：病患（Patient）
* 商業流程編號：BP-RS-04
* 摘要描述：病患檢視歷史與未來之預約紀錄與狀態，包含詳細資訊與可下載收據（若有）。
* 前置條件：病患已登入並為查詢帳號擁有者；系統保存該病患之預約資料。
* 後置條件：系統回傳符合查詢條件的預約清單與詳細資訊；若包含敏感資料需依權限過濾。
* 主要流程：
  1. 病患在個人頁面選擇查看預約紀錄並可用日期篩選。
  2. 系統根據篩選條件與權限回傳預約列表與每筆之詳細狀態（已完成／到診／過號／已取消）。
  3. 病患可選擇下載收據或查看提醒歷程（如有）。
* 替代/異常流程：
  + A1（無權限）：若嘗試查詢非自身或需進階授權之資料，系統拒絕並記錄異常嘗試。
  + A2（資料缺失）：若部份歷史資料缺失或被封存，系統提示並提供申請管道。

flowchart TD  
 Start --> Request[病患提出查詢請求]  
 Request --> Auth[系統驗證身分與權限]  
 Auth -->|允許| Fetch[回傳預約紀錄]  
 Auth -->|拒絕| Deny[回傳存取受限]  
 Fetch --> End  
 Deny --> End

### UC-QM-01 線上報到（Online Check-in）

* 主要動作者：病患（Patient）
* 商業流程編號：BP-QM-01
* 摘要描述：病患於看診前線上報到；系統檢查帳號限制狀態並決定是否允許完成線上報到。
* 前置條件：病患已登入且在報到時間窗內；預約 status 為可報到。
* 後置條件：若允許，病患標示為已報到並加入候診佇列；若受限，報到被阻止並提示改至現場機台。
* 主要流程：
  1. 病患在個人頁面按「線上報到」。
  2. 系統先檢查病患帳號是否為「限制線上報到」。  
     1. 若為限制狀態：阻止線上報到，顯示說明（包括限制原因/剩餘天數/申訴連結）並提示前往現場機台（UC-QM-02）。
     2. 若未限制：系統記錄線上報到，將病患加入候診佇列並通知診間人員。
  3. 系統寫入審計日誌與報到紀錄。
* 替代/異常流程：
  + A1（網路或系統錯誤）：若寫入報到紀錄失敗，提示病患稍後重試或至現場報到；同時記錄錯誤供管理員排查。
  + A2（嘗試繞過限制）：若偵測帳號企圖繞過限制（例如偽造請求），系統阻擋並發出安全警示給管理員。

flowchart TD  
 Start --> Click[病患按線上報到]  
 Click --> CheckRestrict[系統檢查是否限制線上報到]  
 CheckRestrict -->|限制| Block[阻止報到並顯示改至機台訊息]  
 CheckRestrict -->|未限制| Proceed[標記已報到並加入候診]  
 Proceed --> Audit[寫入審計日誌]  
 Block --> End  
 Audit --> Notify[通知診間]  
 Notify --> End

### UC-QM-02 現場機台報到（Kiosk / On-site Check-in）

* 主要動作者：病患（Patient）、現場機台（Kiosk）操作人員（或 Patient 自助）
* 商業流程編號：BP-QM-02
* 摘要描述：病患於現場機台輸入預約資訊完成報到；若預約已被判定為過號，系統將病患插入當前叫號後第三位。
* 前置條件：病患到院並持有效預約或證件；機台連線正常或櫃檯提供人工報到。
* 後置條件：病患完成報到並按規則插入候診序列，系統更新狀態並記錄操作。
* 主要流程：
  1. 病患在機台掃卡或輸入預約編號以識別預約。
  2. 系統核對預約狀態並檢查是否為過號觀察或已被判定為過號。
  3. 若非過號：系統將病患加入候診佇列的末端或按一般規則排序並回傳號碼。
  4. 若為過號或被判定為過號：系統將病患插入到當前叫號後第 3 位，更新序列並寫入操作紀錄（包含機台編號、時間戳）。
  5. 系統顯示並列印號碼，通知診間人員。
* 替代/異常流程：
  + A1（機台離線）：提示機台離線並引導至人工櫃檯；人工報到需管理員介入並寫入相同格式紀錄。
  + A2（預約不存在或已取消）：回傳錯誤並指示聯絡客服或管理員。
  + A3（插隊衝突）：若同時多名過號者嘗試插入位置，系統以原子交易保證順序，並在衝突時以到達時間排序或提示等待。

flowchart TD  
 Start --> Scan[掃卡或輸入預約編號]  
 Scan --> Verify[系統核對預約與狀態]  
 Verify --> |非過號| Normal[正常加入候診]  
 Verify --> |過號| NoShow[插入當前叫號後第3位並記錄]  
 Normal --> Print[回傳號碼並通知診間]  
 NoShow --> Print  
 Print --> End

### UC-QM-03 病患查看候診資訊（View Queue Status / Real-time）

* 主要動作者：病患（Patient）
* 商業流程編號：BP-QM-03
* 摘要描述：病患查看即時候診順位、前方等候人數與預估等待時間，並接收靠近提醒。
* 前置條件：病患已完成報到（線上或現場）或系統能識別該預約序列。
* 後置條件：系統回傳即時候診資訊；若資料不完整則提示最後更新時間。
* 主要流程：
  1. 病患開啟候診頁面或接收推播，系統查詢排隊狀態並回傳順位與預估等待。
  2. 系統持續更新並在靠近時提供提醒（例如前兩名時）。
* 替代/異常流程：
  + A1（資料延遲）：若實時資料延遲或服務降級，系統回傳最後已知狀態並標示可能不準確。
  + A2（隱私限制）：若病患無權查看該序列（例如非本人），系統拒絕並記錄異常。

flowchart TD  
 Start --> Request[病患請求候診資訊]  
 Request --> Query[系統查詢排隊狀態]  
 Query --> Return[回傳順位與預估時間]  
 Return --> Notify[若接近則發送提醒]  
 Notify --> End

### UC-QM-04 即時看診資訊（Clinic Real-time Info / Dashboard View）

* 主要動作者：病患（Patient）、醫護/管理人員（ClinicStaff/Admin）
* 商業流程編號：BP-QM-04
* 摘要描述：提供診間即時運作資訊（當前叫號、候診人數、診間負載）給病患與管理端以提升透明度與運營調度效率。
* 前置條件：診間系統正常上報叫號與候診事件；使用者具備相應檢視權限。
* 後置條件：使用者可檢視即時資訊；管理員可基於資訊進行臨時調配決策。
* 主要流程：
  1. 診間系統或人工操作上報當前叫號或候診變更。
  2. 後端接收事件並更新即時資料流與儀表板。
  3. 病患或管理員透過前端查看即時資訊；系統提供過載或延遲警示（若適用）。
* 替代/異常流程：
  + A1（資料上報中斷）：若診間端未上報，顯示最後已知狀態並標示資料延遲。
  + A2（權限不足）：若使用者無權檢視某些欄位，則隱藏敏感資訊並提示權限不足。

flowchart TD  
 Start --> Report[診間上報叫號/候診事件]  
 Report --> Update[後端更新即時資料流]  
 Update --> Front[前端/儀表板顯示]  
 Front --> End

### UC-EHR-05 審計日誌檢視（Audit Log Search & Export）

* 主要動作者：管理員（Administrator）、合規稽核人員（Auditor）
* 商業流程編號：BP-EHR-05
* 摘要描述：管理員或稽核人員依權限搜尋、過濾與匯出病歷相關操作之審計日誌（CSV/JSON），以支援稽核或法律要求。
* 前置條件：操作者為授權管理員或稽核角色並已登入；系統存在審計日誌資料。
* 後置條件：回傳篩選後的審計日誌並提供下載匯出，所有匯出行為需被記錄。
* 主要流程：
  1. 管理員進入審計查詢介面並設定時間區間、使用者 ID、操作類型等條件。
  2. 系統根據條件檢索審計日誌並回傳結果預覽。
  3. 管理員可選擇匯出格式（CSV/JSON）並執行匯出，系統提供下載並記錄匯出操作（操作者、時間戳、查詢條件）。
* 替代/異常流程：
  + A1（權限不足）：若操作者權限不足，系統拒絕並記錄嘗試。
  + A2（資料量過大）：若查詢結果超過系統限制，系統提示分段下載或改以時間分段查詢。
  + A3（匯出失敗）：若匯出過程失敗（I/O 或權限問題），系統提示錯誤並保留查詢條件以便重試。

flowchart TD  
 Start --> Query[管理員輸入查詢條件]  
 Query --> Search[系統檢索審計日誌]  
 Search --> Preview[回傳結果預覽]  
 Preview --> Export[管理員執行匯出]  
 Export --> Save[系統產生檔案並記錄匯出操作]  
 Save --> End

### UC-EHR-06 存取控管（RBAC: Role-Based Access Control）

* 主要動作者：系統管理員（Administrator）、資安負責人（Security Officer）、系統服務（Service）
* 商業流程編號：BP-EHR-06
* 摘要描述：建立與管理角色與權限，當使用者嘗試存取病歷或敏感欄位時，系統依 RBAC 規則驗證並允許或拒絕存取。
* 前置條件：管理員已登入並有權限管理角色/權限；系統有既定權限矩陣與敏感欄位定義。
* 後置條件：角色與權限變更生效，所有存取嘗試均依新規則進行檢核，變更寫入審計日誌。
* 主要流程：
  1. 管理員在權限管理介面建立/修改角色並分配權限（例如：醫師可讀寫其負責病患；行政僅讀取非敏感欄位）。
  2. 系統儲存權限矩陣並生效。
  3. 當使用者或服務嘗試存取病歷資料時，授權服務根據角色、資源與操作類型（read/write/delete）進行檢查並回傳允許或拒絕。
  4. 系統記錄每次授權決策的審計紀錄（含操作者/服務、時間、被請求的資源與決策原因）。
* 替代/異常流程：
  + A1（緊急權限 / 臨時升權）：管理員可釋出臨時授權（有 TTL）以支援緊急作業，該操作需有二次核准並寫入審計。
  + A2（權限衝突）：若角色變更導致權限衝突或違反政策，系統可拒絕並回報變更差異供審計與人工核准。
  + A3（授權服務故障）：若授權服務短暫不可用，系統應採取安全預設（deny by default）或有限度降級策略，並記錄事件以供回溯。

flowchart TD  
 Start --> AdminChange[管理員建立/修改角色權限]  
 AdminChange --> SavePolicy[系統儲存權限矩陣]  
 SavePolicy --> Enforce[授權服務生效]  
 Enforce --> Access[使用者/服務請求存取資源]  
 Access --> Check[授權服務檢查角色/操作]  
 Check -->|允許| Allow[允許存取並記錄審計]  
 Check -->|拒絕| Deny[拒絕並記錄審計]  
 Allow --> End  
 Deny --> End

### UC-CM-01 掛號結果通知（Send Appointment Confirmation）

* 主要動作者：系統通知服務（Notification Service）、病患（Patient）
* 商業流程編號：BP-CM-01
* 摘要描述：在預約建立或變更後，系統根據通訊模板發送確認通知（Email/SMS/推播）並記錄送達結果。
* 前置條件：預約已建立且病患有可用聯絡方式；通知模板已設定。
* 後置條件：通知發送記錄被寫入審計/通知日誌；若發送失敗，該事件記錄以便重試或人工處理。
* 主要流程：
  1. 預約建立或變更觸發通知事件。
  2. 通知服務根據病患偏好與模板選擇通道（Email/SMS/推播）並發送訊息。
  3. 通知服務記錄送達狀態（成功/失敗/重試中）。
* 替代/異常流程：
  + A1（發送失敗）：若第一次發送失敗，系統依重試策略重試；若仍失敗，標記為失敗並顯示於管理員儀表板以人工處理。
  + A2（聯絡資訊缺失）：若病患無可用聯絡方式，系統標示需人工聯絡並在管理儀表板呈現。

flowchart TD  
 Start --> Trigger[預約建立/變更觸發通知]  
 Trigger --> SelectChannel[選擇通知通道與模板]  
 SelectChannel --> Send[發送通知]  
 Send --> |成功| LogOK[記錄成功]  
 Send --> |失敗| Retry[依重試策略重試]  
 Retry --> |仍失敗| LogFail[記錄失敗並標示給管理員]  
 LogOK --> End  
 LogFail --> End

### UC-CM-02 門診流量儀表板（Clinic Load Dashboard / Admin View）

* 主要動作者：管理員（Administrator）
* 商業流程編號：BP-CM-02
* 摘要描述：管理員查看即時門診流量、診間負載與 KPI，並能匯出報表或下達臨時調度指令。
* 前置條件：後端需有即時資料流與儀表板服務；管理員具有檢視權限。
* 後置條件：管理員獲得即時視覺化資訊並可執行匯出或發送調度通知。
* 主要流程：
  1. 系統聚合來自預約、報到、候診與處置的即時事件，計算關鍵指標（候診人數、平均等待、診間負載）。
  2. 管理員在儀表板檢視並可按時段或科別過濾；如需，匯出報表或發出臨時排班調度通知。
* 替代/異常流程：
  + A1（資料延遲或部分遺失）：系統顯示資料延遲標記並建議重新整理或進行離線查詢。
  + A2（匯出失敗）：若匯出檔案產生失敗，系統提示並允許分段匯出或重試。

flowchart TD  
 Start --> Aggregate[聚合即時事件與計算 KPI]  
 Aggregate --> Display[儀表板顯示]  
 Display --> |匯出| Export[產生報表並提供下載]  
 Display --> |調度| Dispatch[發送臨時調度通知]  
 Export --> End  
 Dispatch --> End

### UC-CM-03 看診提醒通知（Appointment Reminder）

* 主要動作者：系統通知服務（Notification Service）、病患（Patient）
* 商業流程編號：BP-CM-03
* 摘要描述：系統依通知規則在預定時間（例如 48h/24h/2h 前）發送提醒，記錄送達結果並支援多通道。
* 前置條件：預約存在且病患聯絡資訊有效；通知排程已建立。
* 後置條件：提醒發送記錄寫入通知日誌；若送達失敗觸發重試或人工介入。
* 主要流程：
  1. 通知排程器在設定時間點觸發通知事件。
  2. 通知服務根據模板與病患偏好發送通知（Email/SMS/推播）。
  3. 記錄送達結果並在失敗時依策略重試或標示為需人工處理。
* 替代/異常流程：
  + A1（頻率限制）：若通知過度（例如連續多次失敗且迅速重試），系統應採取降頻策略並發出警示給管理員。
  + A2（聯絡方式變更）：若在重試期間病患更新聯絡資訊，系統應使用最新資訊進行下一次重試。

flowchart TD  
 Start --> Schedule[排程器觸發提醒事件]  
 Schedule --> Send[通知服務發送提醒]  
 Send --> |成功| LogOK[記錄成功]  
 Send --> |失敗| Retry[重試策略]  
 Retry --> |重試結束仍失敗| Escalate[標示需人工處理並通知管理員]  
 LogOK --> End  
 Escalate --> End