

電子處方箋資料 QR code

說明文件

壹、	修訂紀錄表.....	2
貳、	作業目的及執行環境說明	3
一、	作業目的	3
二、	執行環境需求	3
參、	作業流程.....	4
一、	作業流程圖	4
二、	流程說明	4
三、	QR code 資料內容格式說明	6
四、	QR code 內容.....	8
五、	開立端產製說明_一般讀卡機	10
六、	開立端產製說明_健保讀卡機	11
七、	調劑端讀取說明_一般讀卡機	12
八、	調劑端讀取說明_健保讀卡機	14
九、	QR code 資料內容格式範例	16
十、	處方箋資料加解密方式說明	19

壹、修訂紀錄表

版本	日期	修改摘要
Beta 版	113/04/10	Beta
V1.0 版	113/08/05	首發
V1.1 版	113/08/07	調整文字說明
V1.2 版	113/09/03	增加醫事人員憑證序號
V1.3 版	113/10/24	增加 QR Code 欄位格式說明
V1.4 版	113/10/25	調整調劑端下載憑證之網址

貳、作業目的及執行環境說明

一、作業目的

提供民眾就醫之處方資料傳遞，藉由讀取 QR Code，避免處方箋遭竄改或重複調劑，以提升用藥安全及品質。

二、執行環境需求

(一) HCA API / HCA CSAPI

產製電子處方箋 QR code 需使用 HCA API / HCA CSAPI，HCA API / HCA CSAPI 使用方法請參考「醫事憑證管理中心 HCA2.0 程式開發人員專屬網站」（<https://hcadevelopers.mohw.gov.tw/Home/Index>）

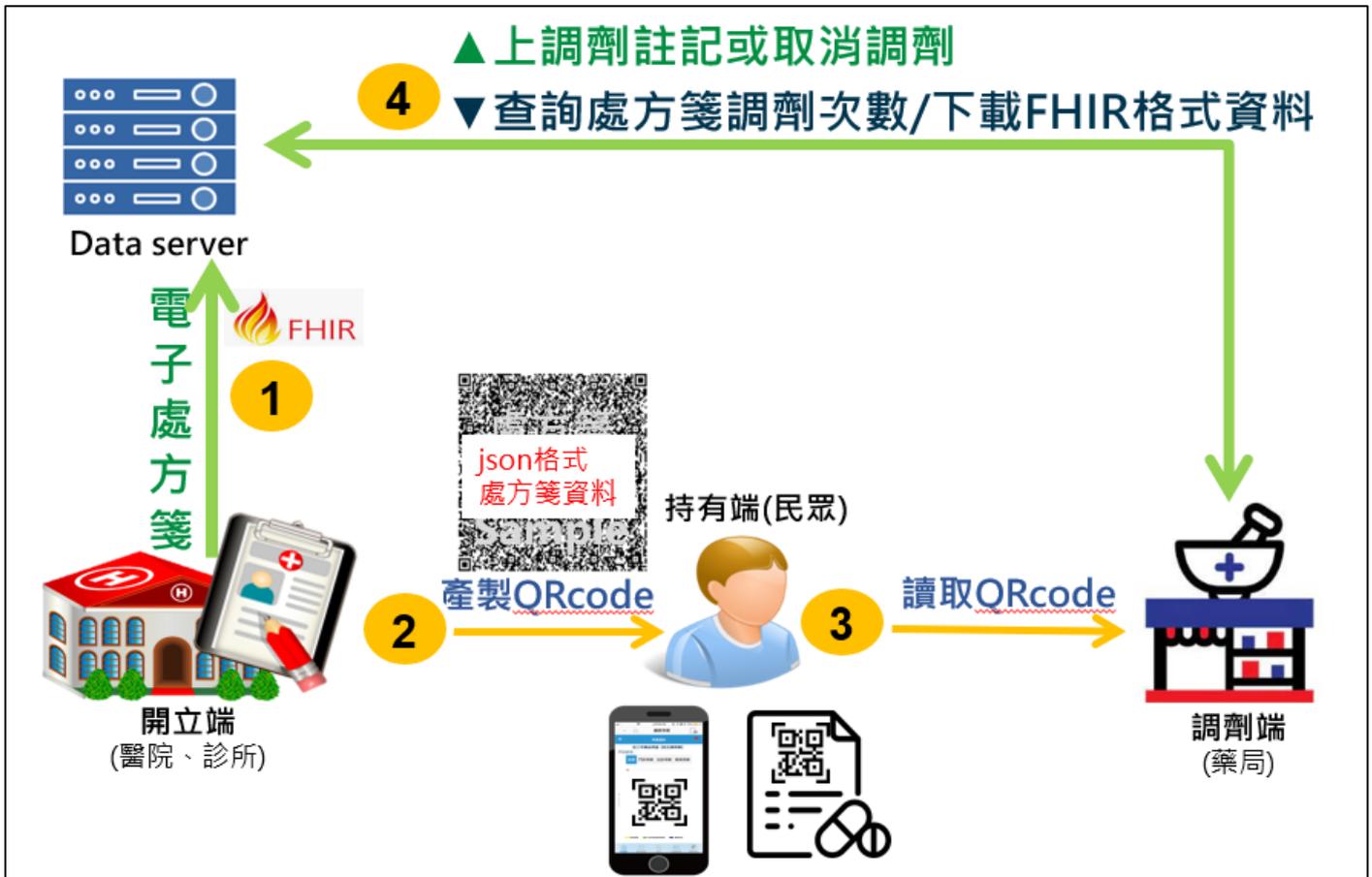
(二) 開立端前置作業

電子處方箋 QR code 之「就醫識別碼」為必填欄位，產製前請先參考下列文件，取得該次就醫之「就醫識別碼」：

1. 本署全球資訊網「就醫識別碼專區-健保卡資料上傳格式 2.0 作業說明」之文件。
2. 本署全球資訊網「健保卡資料下載區-控制軟體 5.1.5.7 版安裝包-CSAPISpec5.1.5.7.pdf」。
3. 本署健保資訊網服務系統（VPN）「下載專區-電腦設定」：
 - (1) Web API—具讀卡機控制軟體相同回傳格式_介接說明書
 - (2) 就醫識別碼 web API 介接說明書
 - (3) 健保資訊網服務系統（VPN）登入服務增值應用元件使用說明書

參、作業流程

一、作業流程圖



二、流程說明

(一) 開立端

1. 完成看診及開立處方，並取得「就醫識別碼」。
2. 將處方箋資料依本文件之規格產製 QR code。
3. 依本文件格式將 QR code 列印於紙本，交付予民眾。
4. 透過本署提供之「電子處方箋開立端 WebAPI 說明文件」上傳 FHIR 格式及 QR Code 內容之電子處方箋，FHIR 相關資訊請參考電子病歷交換單張實作指引(EMR-IG): <https://twcore.mohw.gov.tw/ig/emr/>

(二) 調劑端

1. 掃描處方箋 QR code。
2. 解析 QR code 取得處方箋明細。
3. 透過本署提供之「電子處方箋調劑端 WebAPI 說明文件」上傳調劑註記。
4. 進行調劑作業。

三、QR code 資料內容格式說明

資料是採用 JSON 的格式傳送，欄位資訊參考電子處方箋 IG:

<https://twcore.mohw.gov.tw/ig/emr/EPvsmodel.html>，開立端將電子處方箋的

資料，存放在正確的欄位標籤後面。電子處方箋的欄位分成兩種類別：

(1) 清單類資料：欄位標籤編號 A1~A32，清單類資料不可重複

(2) 醫令類資料：欄位標籤編號 C1~C18，醫令類資料為可重複

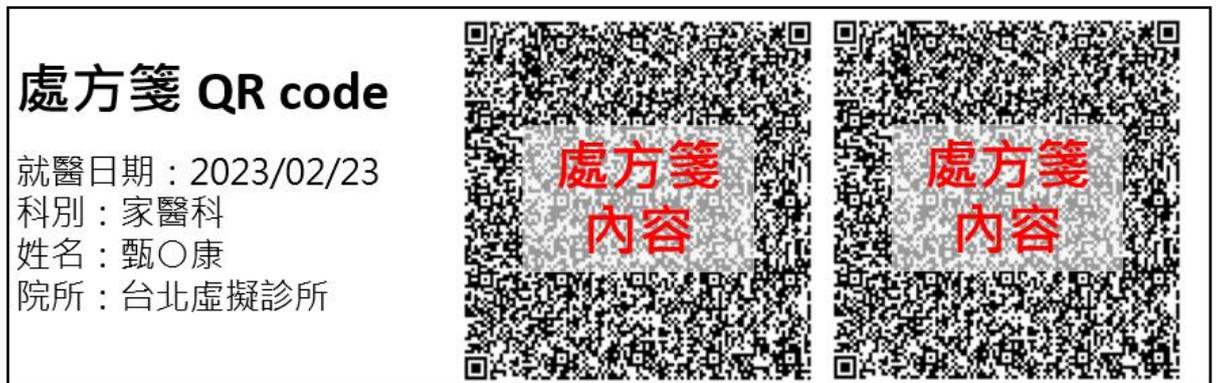
詳細資料範例，請參照：「九、QR code 資料內容格式範例」

項次	描述	欄位名稱	處方箋代碼	格式
1	醫療機構 基本資料	醫療機構代碼	A1	V(10)
2		醫療機構名稱	A2	V(100)
3		醫療機構地址	A3	V(200)
4		醫療機構電話	A4	V(20)
5	病人基本 資料	身分證號	A5	V(10)
6		病歷號碼	A6	V(10)
7		姓名	A7	V(60)
8		性別	A8	V(7)
9		出生日期	A9	D(8)
10		就診年齡	A10	N(3)
11		就醫身分別	A11	V(32)
12		體重	A12	N(5,1)
13	門診基本 資料	門診日期	A13	D(8)
14		科別	A14	V(2)
15		就醫識別碼	A15	V(20)
16		部分負擔代碼	A16	V(3)
17		健保卡就醫序號	A17	V(4)
18		案件分類	A18	V(2)
19		給付類別	A19	V(1)
20	醫事人員 基本資料	醫師姓名	A20	V(60)
21		管制藥品使用執照號碼	A21	V(30)
22		醫師聯絡電話	A22	V(20)
23		醫事人員證書字號	A23	V(30)
24	診斷內容	國際疾病分類代碼	A24	V(9)
25		醫療評估內容註記	A25	V(64)
26		處方箋單號	A26	V(64)
27		處方箋種類註記	A27	V(1)
28		須被合併之處方箋註記	A28	V(1)
29		處方箋有效日期	A29	D(8)
30		處方箋註銷註記	A30	V(1)
31		給藥總日份	A31	N(3)
32		連續處方可調劑次數	A32	N(2)

項次	描述	欄位名稱	處方箋代碼	格式
33	處方內容	醫令類別	C1	V(1)
34		項次	C2	V(2)
35		健保代碼	C3	V(12)
36		藥品商品名稱	C4	V(600)
37		學名	C5	V(600)
38		不得以其他廠牌藥品替代之理由	C6	V(800)
39		藥品單位含量	C7	N(11,3)
40		劑型	C8	V(22)
41		劑量	C9	N(11,3)
42		劑量單位	C10	V(6)
43		頻率	C11	N(10)
44		使用時間	C12	V(38)
45		給藥途徑	C13	V(8)
46		給藥日數	C14	N(3)
47		給藥總量	C15	N(6,2)
48		給藥總量單位	C16	V(10)
49		自費註記	C17	V(1)
50		用藥指示	C18	V(9)

四、 QR code 內容

(一) QR code 及紙本列印格式



1. 處方箋 QR code 包含以下顯性資料：
 - (1) 就醫日期
 - (2) 就醫科別：請以中文名稱供民眾辨識
 - (3) 病人姓名：請以○遮蔽
 - (4) 開立院所名稱
2. 1...N 個 QR code 內資料包含醫事人員憑證序號、醫事人員數位簽章資料及電子處方箋 JSON 格式資料
3. 列印之最小尺寸：3.75 公分 × 3.75 公分
4. 需使用雷射印表機進行列印
5. QR code 規格：
 - (1) 版本(Version)：29
 - (2) 錯誤修正等級(Error Correction Level)：L (7%)
 - (3) 模組(modules)：2 點
6. 如處方箋內容超過可容納範圍（1628 Bytes），請依處方箋 QRCode 內容格式，新增 QR code。

(二) 處方箋 QRCode 內容格式

1. 須包含 3 個標籤：C、S 及 D1。
2. C：醫事人員憑證序號
3. S：Base64 Encode 醫事人員數位簽章資料。
4. D1：Base64 Encode 電子處方箋 JSON 格式資料。
 - (1) 中文編碼請使用 UTF-8。
 - (2) 欄位內容請參考「三、QR code 資料內容格式說明」。
 - (3) 採用 JSON 格式，以 Brotli 壓縮方式壓縮，再使用 AES256 將資料加密，最後再用 Base64 進行編碼(Encode)。
 - (4) 加密方式說明請參閱「十、處方箋資料加解密方式說明」
5. 將 C 憑證序號、S 數位簽章及 D1 處方箋資料結合，如 C+S+D1 總長度超過 1628 Bytes，請將「處方箋資料」拆成 2 段，第 2 段標籤以「D2」存放至新增之 QR code。

- 處方箋 QRCode 資料，未超過 1628 Bytes(一顆 QR Code)

```
{"C": "...憑證序號...", "S": "...Base64 Encode 數位簽章...", "D1": "...Base64 Encode 處方箋資料..."}
```

- 處方箋 QRCode 資料，超過 1628 Bytes(超過一顆 QR Code)

```
{"C": "...憑證序號...", "S": "...Base64 Encode 數位簽章...", "D1": "...Base64 Encode 處方箋資料(第 1 段)..."}
{"D2": "...Base64 Encode 處方箋資料(第 2 段)..."}

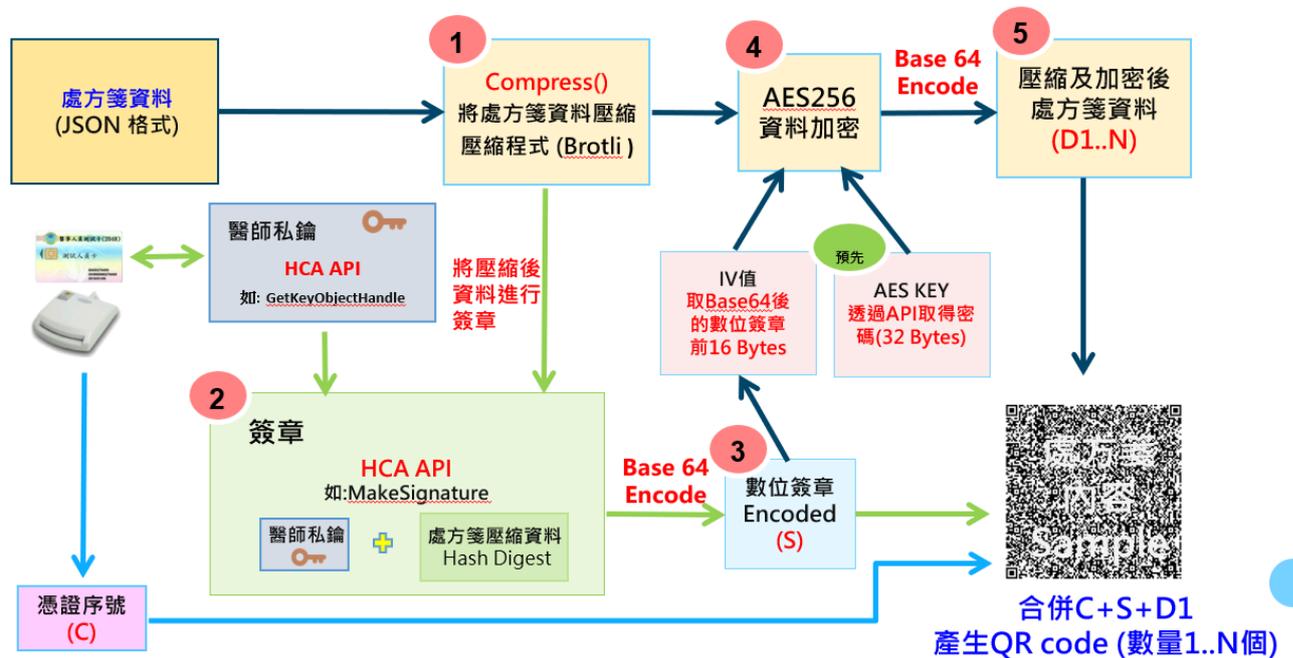
```

```
{"D2": "...Base64 Encode 處方箋資料(第 2 段)..."}

```

五、開立端產製說明_一般讀卡機

開立端產製處方箋QR code流程(一般讀卡機)



(一) 由簽章憑證取得 C 醫事人員憑證序號

(二) 產製 S 數位簽章之內容

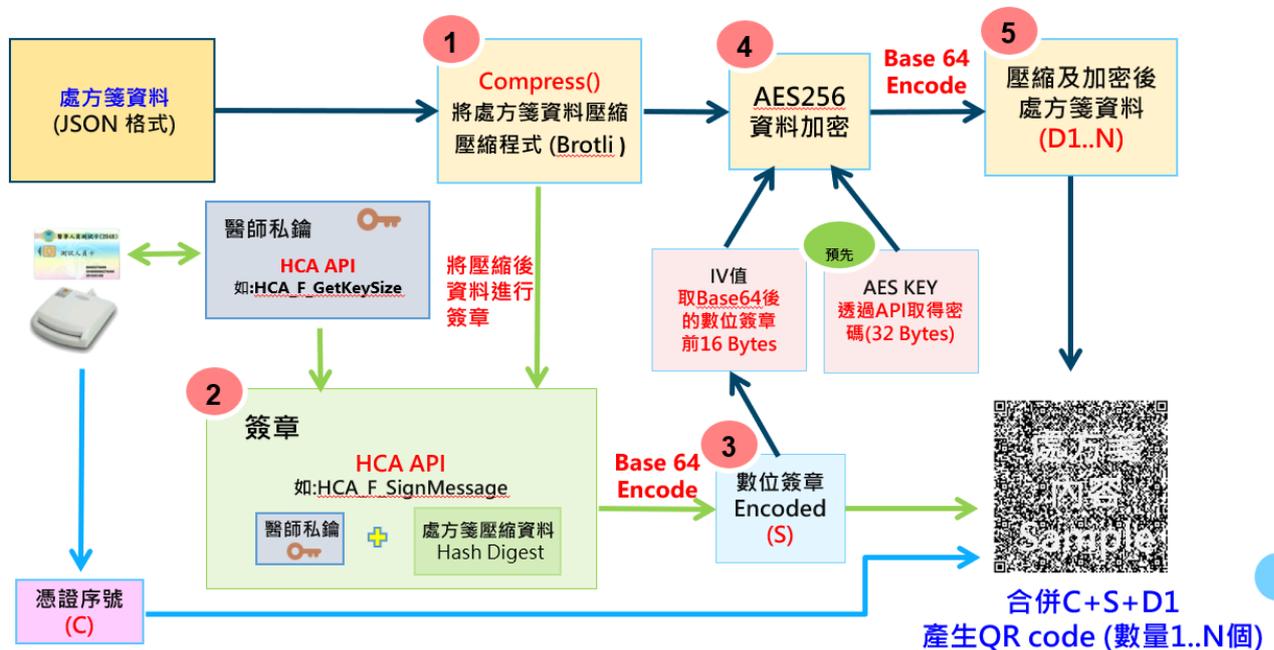
1. 使用 HCA API 取得醫師私鑰(GetKeyObjectHandle)。
2. 使用 HCA API 將處方箋資料簽章(MakeSignature：以預設的 CKM_SHA1_RSA_PKCS 方式，由 HCA API 產生處方箋資料 Hash Digest)。
3. 將簽章資料以 Base 64 編碼後完成 S 數位簽章。

(三) 產製 D1 處方箋資料之內容

請參考「四、QR code 內容-(二)處方箋 QRCode 內容格式」說明。

六、開立端產製說明_健保讀卡機

開立端產製處方箋QR code流程(健保讀卡機)



(一) 由簽章憑證取得 C 醫事人員憑證序號

(二) 產製 S 數位簽章之內容

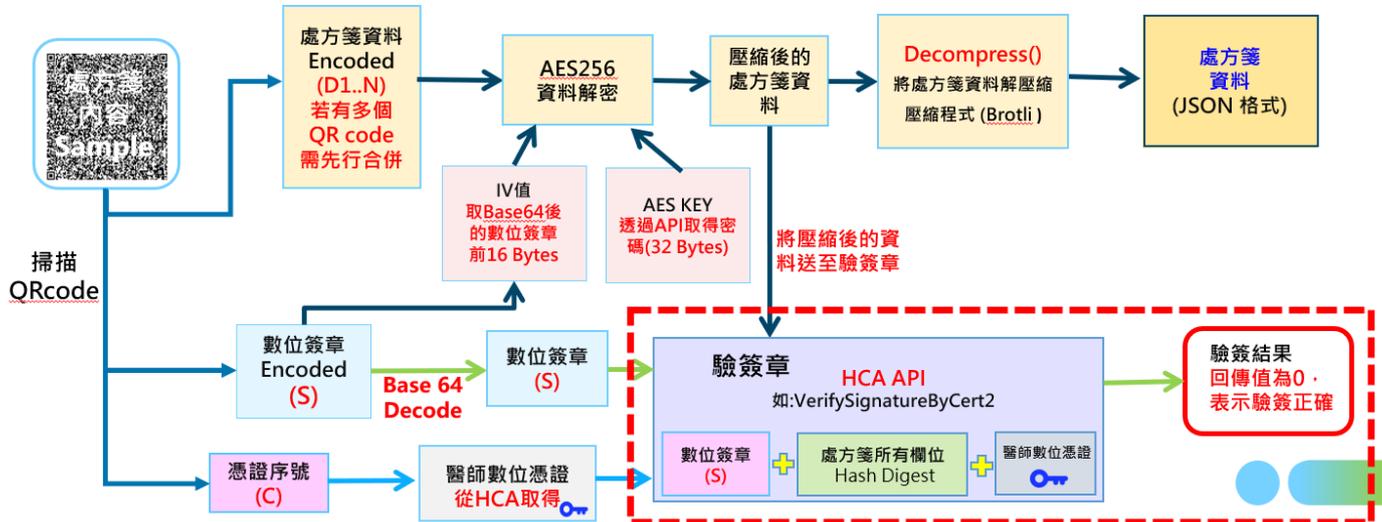
1. 使用 HCA CSAPI 取得醫師私鑰長度(HCA_F_GetKeySize)。
2. 使用 HCA CSAPI 將處方箋資料簽章(HCA_F_SignMessage：由 HCA CSAPI 以 sha1withRSA 簽章演算法產生處方箋資料 Hash Digest)。
3. 將簽章資料以 Base 64 編碼後完成 S 數位簽章。

(三) 產製 D1 處方箋資料之內容

請參考「四、QR code 內容-(二)處方箋 QRCode 內容格式」說明。

七、調劑端讀取說明_一般讀卡機

調劑端讀取處方箋QR code流程(一般讀卡機)



(一) 處方箋資料

1. 掃描 QR code，並解析出醫事人員憑證序號(C)、數位簽章(S)及處方箋資料(D1)。
2. 將處方箋資料(D1)以 Base64 解碼取得處方箋加密壓縮資料。
3. 使用 AES256 解開加密壓縮處方箋資料，解密方式說明請參閱「十、處方箋資料加解密方式說明」
4. 再將解密後處方箋資料，透過壓縮程式(Brotli)，進行解壓縮，取得 JSON 格式處方箋資料。

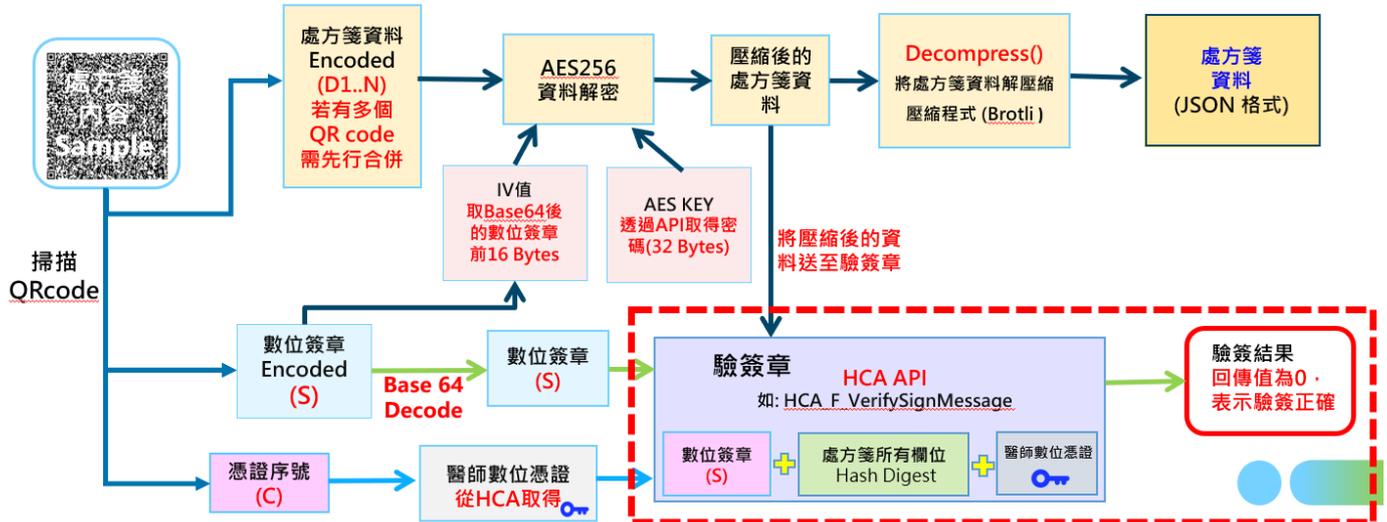
(二) 驗簽章

1. 以憑證序號透過 HCA 服務網址：
<https://10.241.176.234/DownloadCert?CertNo=0300XXXXXXXXXXXXXXXXXA0000001Q065Q>(憑證序號)，取得醫師數位憑證。
2. 以「醫師數位憑證」、「Base64 解碼之數位簽章」及「壓縮後之處方箋資料」，使用 HCA API 驗簽(VerifySignatureByCert2：由 HCA API 產生

處方箋資料 Hash Digest)，如回傳值為 0，表示驗簽正確。

八、調劑端讀取說明_健保讀卡機

調劑端讀取處方箋QR code流程(健保讀卡機)



(一) 處方箋資料

1. 掃描 QR code，並解析出醫事人員憑證序號(C)、數位簽章(S)及處方箋資料(D1)。
2. 將處方箋資料(D1)以 Base64 解碼取得處方箋加密壓縮資料。
3. 使用 AES256 解開加密壓縮處方箋資料，解密方式說明請參閱「十、處方箋資料加解密方式說明」
4. 再將解密後處方箋資料，透過壓縮程式(Brotli)，進行解壓縮，取得 JSON 格式處方箋資料。

(二) 驗簽章

1. 以憑證序號透過 HCA 服務網址：
<https://10.241.176.234/DownloadCert?CertNo=0300XXXXXXXXXXXXXXXXXA0000001Q065Q> (憑證序號)，取得醫師數位憑證。
2. 以「醫師數位憑證」、「Base64 解碼之數位簽章」及「壓縮後之處方箋資料」，使用 HCA CSAPI 驗簽(HCA_F_VerifySignMessage：由 HCA

CSAPI 產生處方箋資料 Hash Digest)，如回傳值為 0，表示驗簽正確。

九、 QR code 資料內容格式範例

```
{  
  "A1": "3501200000",  
  "A2": "台北虛擬診",  
  "A3": "臺北市大安區信義路三段 140 號",  
  "A4": "02-27065866",  
  "A5": "Z299999965",  
  "A6": "D123456",  
  "A7": "甄小莉",  
  "A8": "male",  
  "A9": "2000-01-01",  
  "A10": "51",  
  "A11": "健保",  
  "A12": "50",  
  "A13": "2024-01-01",  
  "A14": "01",  
  "A15": "01234567890123456789",  
  "A16": "001",  
  "A17": "0001",  
  "A18": "01",  
  "A19": "1",  
  "A20": "甄大莉",  
  "A21": "M0000558",  
  "A22": "02-27065866",  
  "A23": "D987654123",  
  "A24": "A01",  
  "A25": "無",  
  "A26": "Med0000001",  
  "A27": "A",  
  "A28": "否",  
  "A29": "2024-01-01",  
  "A30": "N",  
  "A31": "7",  
  "A32": "1",  
  
  "medication": [  
  
    {
```

```

    "C1": "1",
    "C2": "1",
    "C3": "B013249100",
    "C4": "旺爾華軟膠囊 0.5 微公絲",
    "C5": "ALFACALCIDOL",
    "C6": "",
    "C7": "0.5",
    "C8": "TAB",
    "C9": "1.0",
    "C10": "顆",
    "C11": "1",
    "C12": "QOD",
    "C13": "PO",
    "C14": "3",
    "C15": "2",
    "C16": "顆",
    "C17": "N",
    "C18": "無"
  },
{
    "C1": "1",
    "C2": "2",
    "C3": "BC21571100",
    "C4": "脈優錠 5 毫克",
    "C5": "AMLODIPINE",
    "C6": "",
    "C7": "5",
    "C8": "TAB",
    "C9": "1.0",
    "C10": "顆",
    "C11": "1",
    "C12": "QD",
    "C13": "PO",
    "C14": "3",
    "C15": "3",
    "C16": "顆",
    "C17": "N",
    "C18": "無"
}
]

```

}

十、處方箋資料加解密方式說明

為強化資訊安全，針對敏感性資料採行進階加密標準（Advanced Encryption Standard, AES）演算法以 256 位元的金鑰長度來處理電子處方箋內資料的加密，保障民眾的個人隱私資料的安全。

電子處方箋 AES 加解密之設定參數說明如下：

「MODE」：設定為"CBC"

「Padding」：設定為"PKCS#7"

「加解密 KEY」：KEY 值為 256 bits，透過 API 取得 32 Bytes 的固定長度字串轉換為 KEY 值。固定長度字串的取得，透過 API 由健保署提供。詳細說明請參閱「電子處方箋開立端 WebAPI 說明文件」/「電子處方箋調劑端 WebAPI 說明文件」。

「IV 值」：將電子處方箋資料壓縮後，做成電子簽章，並且經過 Base64 編碼過後，取前 16 Bytes 作為本次加密之 IV 值。

以下圖為例：S 標籤資料取出前 16 Bytes 資料" **NxWEKoi0n5fpHGHV**"，作為本次加密之 IV 值。解密時取得 QRcode 資料後，將 QRcode 內 S 標籤資料取出前 16 Bytes 資料，作為解密時所使用之 IV 值。

```
{"S":"NxWEKoi0n5fpHGHVcetF.....","D1":"eWEwBRMT6T0ZF1C1H3TL9qaRYUI0....."}
```