作業報導

● 中央健康保險局醫療資料實體加密簡介

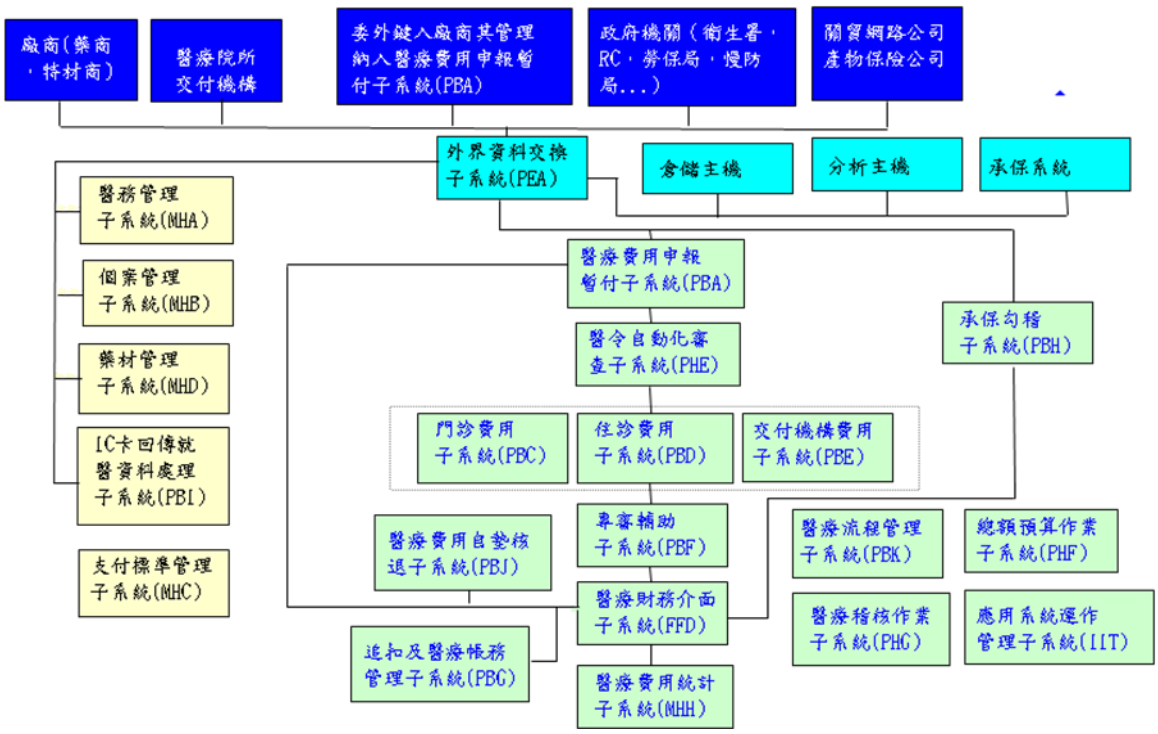
壹、前言

中央健康保險局(以下簡稱「本局」)各級長官均非常重視資通安全，對於各項資通安全機制導入不遺餘力。本局不僅建置各項軟、硬體機制，包括：病毒防範、防火牆、入侵防禦系統、弱點偵測系統、傳輸加密機制；另一方面也建立各類的權限管理、各項資安程序及辦法，並導入 ISMS，通過 ISO27001 認證。雖然，以上這些軟、硬體機制對資安有相當程度的強化作用，但本局重要之醫療電子資料爲民眾就醫紀錄，其資料特性具有高度機敏性，若有資料外洩，將造成國家、社會重大的不安，爲能更有效並徹底保護最重要的資產─醫療資料，本局研擬醫療資料實體加密，以高強度的加密技術，對重要的資料欄位以亂碼處理，對資料做更徹底的保護，當外界特約醫療院所向本局申報資料時，在匯入本局後立即予以加密，儲存於資料庫，無論本局內部人員、外部人員或網路服務均以加密資料庫爲對象，以確保資料使用的安全，避免機敏資料遭人竊取，大幅降低資料外洩的風險。

貳、資料特性

本局每月接收各特約醫療院所醫療費用申報資料，涉及就診、疾病、費用及處方等多面向資料，具高度機敏性與隱私性，且包含每一國民就醫紀錄，資料量龐大，例如，每月門診申請案件多達 2,900 餘萬件，醫令件數約 1 億 6,500 萬筆；每月住診申請案有 26 餘萬件，醫令約 1,700 餘萬筆。

醫療資訊系統示意圖如下：



參、資料實體加密大事記

本局醫療資料實體加密自民國 97 年開始推動，由於醫療系統非常龐大，包含 20 幾個子系統，程式約一萬支，資料量超過 20TB，加上內部使用者超過 1,500 人，外部使用者更有 2 萬多名特約院所相關人員，因此，整個過程先經過縝密規劃，再選擇一個分區先由資訊面進行試辦，再就業務面評估，最後才全系統進行調整，過程極為繁複，幸賴高階主管全力支持，方得以完成。

推動過程：

辦理階段	辦理情形
醫療資料採實體加密方式來保護 97.05.05	1.資通安全委員會通過醫療資料採實體加密方式來保護。 2.指派南區分局進行實驗與試辦。
資訊技術面評估階段 970505～980119	98 年 1 月 19 日資通安全委員會，由南區針對資訊專業技術面專題報告「醫療系統加密與後續管控措施之研究」。
業務作業面評估階段 980119-980420	98 年 4 月 20 日資通安全委員會，南區針對作業面專題報告「支出面資料加密作業評估報告」。
第一階段實際環境測試 980508～980709	1.98 年 5 月 8 日進行第一階段測試。 2.98 年 5 月 12 日資訊處以 10 支程式建置縮小版模擬平台。 3.98 年 6 月初完成模擬平台之建置，將測試院所申報資料匯入模擬平台。
第二階段實際環境測試 981015～981204	1.98 年 10 月 15 日進行第二階段測試， 測試資料：2 家院所、2 個 ID、PBG 報列呆帳測試。 2.98 年 10 月 16 日及 12 月 4 日，南區回復測試結果及建議，確認其可行性。
確立實體加密原則 990607	簽奉　局長核可醫療資料 5項加密原則。
應用系統畫面及報表進行敏感性資料之遮蔽處理 990608～1000320	針對整個醫療資訊系統請業務單位人員逐一檢視那些畫面報表，在業務上需有明文(沒有任何遮掩)才能處理，計有 219 個畫面與 221 份報表(全部作業畫面 655 個；報表 860 張)。
全系統進行資料實體加密作業 991101～1000701	修改相關批次程式(計有 198 支)，使程式可併行處理資料庫中 ID 資料同時存在有加密及無加密資料。
資料轉換及上線 991101～1000701	以上班時間服務不中斷為前提，擬定轉檔及上線計畫，並針對所有需加密之 333 個資料庫表格，依其費用月分逐步轉檔。

肆、資料加密與資料遮蔽原則：

一、 民眾身分證字號自外界轉入本局即進行加密處理。

二、 針對敏感性資料，如身分證字號、姓名等，所產製之報表及應用系統畫面，預設顯示方式皆採部分遮蔽方式處理如下（詳如附圖一、二）：

身分證字號於應用系統畫面與報表預設顯示方式：

顯示方式	欄位顯示值	說明
部分遮蔽： 解密後遮掩第 5~7 碼(身分證最後 1 碼爲檢查碼故無需遮掩)。	A123***789	畫面或程式可選擇明文顯示功能，並保留執行紀錄。

姓名於應用系統畫面與報表預設顯示方式：

採取中文名字中間字以○代替、英文名字則在第 3~8 碼以*代替

姓名組合	欄位顯示值
姓名爲中文 2 個字	黃○
姓名爲中文 3 個字	黃○明
姓名爲中文 4 個字	黃○○明
姓名爲英文字	第 3~8byte 以半型*顯示

三、 加密採安全 DES 演算法，範圍爲醫療申報資料及醫療上傳資料中具敏感性的相關檔案。

四、 針對部分涉及民眾臨櫃或需與特約醫療院所有互動需求作業而須以明文顯示者，額外開發程式對加密資料進行解碼，俾使業務正常推動。

五、 對於同仁使用解碼以取得明文資料，將建立完整的使用者紀錄。

伍、資料實體加密機制說明

一、 茲將本局現有加解密機制及 survey 參考其它有關資料庫加密處理之技術，進行可行性評估及分析後，採 Oracle 的 DBMS_OBFUSCATION_TOOLKIT 提供的 DES 加解密演算法之 API，撰寫建置於 Oracle DB 加解密的 Stored Function。

二、 將加解密機制寫成 Stored Function，對於應用程式之影響最小，只需在原有 SQL 程式中有關隱密性欄位加上呼叫該 Stored Function 作轉換即可，此方式之執行效率經過測試亦較好。

三、 加密後的字元組無特殊符號或空白鍵，因此不會對應用程式產生干擾。

四、 安全性較高，DES 加密演算法是經過美國政府認可使用的一種加密機制，在注重資料保護的金融界中亦常被應用。

五、 加密後欄位的長度會變長，其 output 長度 = 無條件進位(input 資料的長度/8)*8*2，但相對的提供較高的安全性。

六、 本程式爲安全起見，金鑰密碼採多人分持方式，並依此分持密碼產製 DES 加解密的 stored function SQL，且該 SQL 程式亦經加密處理，故無法由該 SQL 程式得知金鑰密碼，確保其安全性；另爲進一步確保資料安全，區分對外與對內主機採取不同金鑰之加解密函式，以避免對外主機資料庫遭遇攻擊或竊取，亦無從對應內部主機資料庫，俾降低資安事件造成之衝擊。

七、 建立完整的加密資料解密制度，本局各單位人員若有業務需要，如：需請特約醫療院檢送病歷資料等必要作業需要時，本局業務承辦人員可申透電子表單經其主管同意後，由加解密專責窗口提供解密資料，俾便其業務推動，估計需解密資料約佔整體 4.09%。(詳附圖三)

八、 建立完整的加解密函式使用紀錄，透過這些紀錄產製各種使用紀錄及表報，請本局各單位人員進行相關稽核。(詳附圖四)

陸、經驗分享與未來展望

一、必須得到最高主管的支持：由於進行資料實體加密除需將資料庫資料亂碼化，同時要對現有系統進行大幅度的修改，這對現行業務流程及作業方式均產生某種程度的改變，這不但涉及到內部人員，也會影響到外部顧客，若未得到最高主管的支持，很難持續推動。

二、必須有效化解業務單位的抗拒與反彈：由於現行的機敏性資料均是明文，實體加密後變成部分遮蔽，先等到案件審查到必要時，依作業權限查詢明文的畫面報表，或再依程序申請解密，會造成業務單位的反彈，因此如何找出需明文的作業，有效的提供更便利的功能讓他們的不便能降到最低的程度，才能讓這項作業能推動下去。依本局業務進行分析，真正需要依加密前(明文)資料來進行審查追蹤通知等作業需要，僅佔整體 4.09%, 在這個專案中，我們開發明文的畫面及報表各 200 多支程式，使其不便利性降到承辦人員能接受之程度。

三、落實管控提升資料保護力：對於明文資料之使用，必須留下完整紀錄，並產製紀錄統計及分析表報，供其主管瞭解，並作爲日後內部稽核之參考。

附圖一：資料遮蔽畫面範例

應用系統畫面針對敏感性資料作遮蔽—若因業務需要亦可透過明文查詢按鍵顯示明文，系統並同時將該查詢寫入稽核紀錄檔中。

附圖二：資料遮蔽表報範例

相關系統報表針對敏感性資料作遮蔽—

行政院衛生署中央健康保險局 － 臺北業務組

住院醫療費用清單

程式代號：PBDB3013R01　　列印日期：101/09/03

醫事機構：[redacted]　醫事類別：22 住診西醫醫　費用年月：101/01　申報類別：1-送核　申報日期：101/02/14　頁　次：1

科別：醫療費用一科　姓　　名：[redacted]

醫院代號及名稱	費用年月	案件分類	申報類別	流水編號	部分負擔
[redacted]	101/01	Tw-DRGs	送核	13	000

姓名	身分證編號	出生日期	給付類別	交通事故	就醫序號	就醫科別
樂○琬	C220***180	070/09/01	普通疾病	N	0002	直腸外科

入院日期：101/01/18　矯正機關代號：
出院日期：101/01/19　主診斷碼：5651　肛門　管
申報起日：101/01/18　次診斷一：4555　外痔，伴有其他併發症
申報迄日：101/01/19　次診斷二：4552　內痔，伴有其他併發症者
急性病床：1 日　次診斷三：
慢性病床：0 日　次診斷四：
病患來源：1 (1-9.N.R.C.S)　主手術碼：4912　肛門　管切除術
醫師代碼：R120382526　次手術一：4946　痔瘡切除術
DRG 代碼：　次手術二：4523　大腸鏡檢
外因碼一：　次手術三：
外因碼二：　次手術四：
轉診代碼：3　醫令健數：54　依附就醫新生兒胞胎註記：
IC卡資料比對：　TW-DRGs碼：15802　Tw-DRG支付型態：0
就醫新生兒出生日期：　不適用Tw-DRGs案件特殊註記：0
轉入服務機構代號：　轉出服務機構代號：
審查通知事項：

1.請檢送本次住院期間病歷影本或正本
2.請檢送全卷病歷影本或正本
3.請檢送_____檢查報告
4.請檢送_____X片
5.請檢送放射線診療癌症治療記錄
6.請檢送_____治療處置記錄
7.請檢送手術記錄及麻醉記錄
8.請檢送復健治療記錄
9.請檢送血液透析記錄
10.其它

次診斷碼（五～十九）：
次手術碼（五～十九）：

醫療費用	不回推核減	回推核減
診察費： 514		
病房費： 973		
管灌飲食費： 0		
檢查費： 3,844		
放射線診療費： 0		
治療處置費： 77		
手術費： 10,190		
復健治療費： 0		
血液血漿費： 0		
血液透析費： 0		
麻醉費： 2,550		
特殊材料費： 235		
藥費： 588		
藥事服務費： 132		
精神科治療費： 0		
注射技術費： 75		
嬰兒費： 0		
代辦部份負擔： 0		
醫療費用合計： 19,178		
部分負擔金額： 1,918		
申請費用金額： 20,573		

急性病床	醫療費用	部分負擔	慢性病床	醫療費用	部分負擔
30日以內：	19,178	1,918	30日以內：	0	0
31至60日：	0	0	31至90日：	0	0
61日以後：	0	0	91至180日：	0	0
			181日以後：	0	0

附圖三：申請解密爲明文之申請作業

針對含加密身分證字號檔案申請解密之電子需求表單—

資料提供需求單 - 行政院衛生署中央健康保險局 所提供的 Windows Internet Explorer

承辦單位			
需求編號：	P101010035	申請日期：	2012/01/05 17:00
申請單位：	中區駐區資訊人員	申請人員：	[redacted]
聯絡電話：	6082	案件編號：	
資料類別：	資料加解密	希望完成日：	2012/01/09
需求原因及適用法條簡述：	爲提供執行醫療查核業務,申請檔案批次解密處理 sel_hp_c001_10011.txt		

需求內容	
資料條件：	檔案以,爲分隔符號
資料欄位：	第2欄ID欄位解密
提供方式：	其他(PXXT0802下載)
其他描述：	申請人： 通知主管：
資料處理：	不加密 (統計,明細)
資料加/解密：	
使用單位：	局內(中區業務組)
合理期望完成日期：	2012/01/09

承辦人處理資訊									
承辦人	資料筆數	加密	提供欄位	完成日期	提供日期	提供方式	SA	PG	Total
[redacted]	98	否	個人ID	2012/01/09	2012/01/09	電子表單通知下載	0	1	1

處理結果			
承辦科室	承辦人	處理日期	處理結果說明
資訊組醫療資訊科	[redacted]	2012/01/09	利用Med2醫療系統執行完成

附圖四：每月系統自動將彙總各單位申請解密記錄稽核報表 mail 給相關主管

寄件者: [redacted]　　寄件日期: [redacted]
收件者: [redacted]
副本:
主旨: 醫療資訊系統解密記錄稽核報表(100/11)

訊息　[redacted]6.txt (2 KB)

長官好:
附檔定期提供各單位主管其相關同仁執行醫療資訊系統解密作業紀錄
請督導及稽核同仁共同執行本局之資訊安全政策。

**********資安宣告**********
依據個人資料保護法第 28 條規定：
一、公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用
　　或其他侵害當事人權利者（如資料外洩），負損害賠償責任。
二、每一事件受害當事人每人可求償新臺幣五百元以上二萬元以下;
　　每事件賠償總額以新臺幣二億元為限。
同仁應依個人資料保護法及相關法令之規定處理個人資料，並善盡保
管維護之責，若有違失本局將依法究責。
****

附檔解密記錄稽核報表內容

行政院衛生署中央健康保險局 － 臺北業務組
程式代號：PXXH0803R01　　醫療資訊系統解密記錄稽核報表　　頁　次：　1

執行時間:101/08/01~101/08/31
製表日期:101/08/31

申請人	解密需求檔案名稱	解密檔案筆數	執行時間	檔案下載時間	執行備註(需求單編號)
許[redacted]櫻([redacted])	12730P9x19m.csv	6,590	101/08/01	101/08/01	PB101070078
許[redacted]櫻([redacted])	1287e839UD.csv	1,910	101/08/08	101/08/08	PB101080013
許[redacted]櫻([redacted])	12816zsimKZ.csv	4,256	101/08/17	101/08/17	PB101080041
許[redacted]櫻([redacted])	1010822-B110197-2505.csv	2,506	101/08/24	101/08/24	需求編號：PB101080060
許[redacted]櫻([redacted])	1010822-B110197-4971.csv	4,972	101/08/24	101/08/24	需求編號：PB101080060
許[redacted]櫻([redacted])	1010822-B110197-4971.csv	4,972	101/08/24	101/08/24	需求編號：PB101080060
許[redacted]櫻([redacted])	12810QiZAZ9.csv	1,436	101/08/10	101/08/10	PB101080022

（本文由行政院衛生署中央健康保險局資訊組李國隆　提供）