議題2. 維護民眾隱私確保網路應用安全

2.2電子病歷安全

行政院衛生署

2009年8月19日

大綱

一、施政願景

二、現況分析

三、發展趨勢

四、具體策略

五、行動方案

六、討論題綱

電子病歷的核心價值

- 提升醫療品質與病人安全，減少醫療疏失發生。
- 減少重複檢驗、檢查、用藥，提升醫療資源運用效能。
- 節省實體病歷儲存空間，減少環境污染。
- 簡化行政事務作業流程，降低醫院醫務管理成本。
- 有助於醫學研究、教學、統計及分析。

一、施政願景

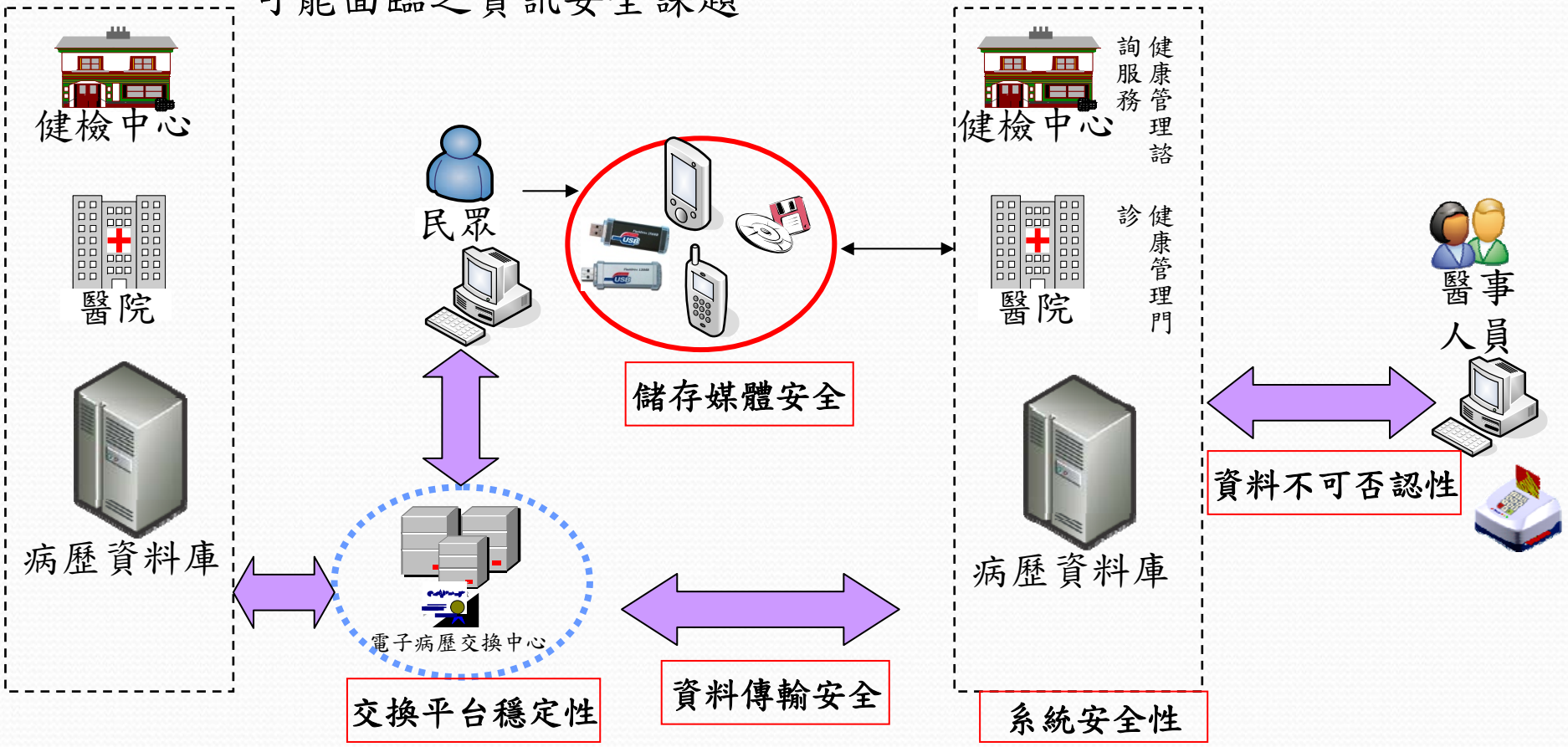
- 建立及維護電子病歷安全，保護病人之隱私，使病人可在任一家醫院，透過健保IC卡，在病人同意下，由經授權之醫師完整取得病人過去之病史資料，提供連續性的照護。

二、現況分析(I)—電子病歷之資安議題

	製作及讀取過程	儲存管理面	交換共享過程
機密性	• 病人隱私受侵犯 • 病人無法對電子病歷之讀取做授權	• 未經授權之病歷資料存取 • 媒體遺失或遭竊取	• 資料傳輸遭攔截 • 未經病人授權 • 病人無電子簽章對電子病歷授權
完整性/不可否認性	• 無法鑑別製作者 • 病歷遭偽造或竄改	• 病歷遭偽造、竄改或刪除	• 病歷遭偽造或竄改 • 無法鑑別收送者
可用性	• 資料操作錯誤 • 系統中斷 • 時戳或簽章之速度緩慢	• 醫事人員作業疏失 • 資料庫毀損 • 系統中斷	• 無法持續運作 • 網路遭駭客攻擊及破壞

二、現況分析

電子病歷的特性：易查詢、易攜帶、易儲存、易傳播、易複製，可能面臨之資訊安全課題



二、現況分析(II)—電子病歷關係人之疑慮

	實施後可能發生之疑慮
顧客面 (病人或社會大眾)	●個人隱私可能被揭露。 ●個人資料可能會被不當蒐集及利用。 ●電子檔可複製性高，資料遭竊取或竄改。 ●電子病歷之使用未規範權限。 ●無電子病歷簽章憑證行使同意權。
醫院及醫護人員	●實施電子病歷會改變工作習慣，可能影響看診進度。 ●產生不必要的醫療糾紛。 ●資料外洩將涉及病人隱私與法律訴訟。 ●電子病歷若因資安而無法運作，嚴重者甚至危及病患生命安全。
專業人士 (資訊專家及廠商)	●電子病歷存取控管不當。 ●系統設計漏洞。 ●內部員工惡意竊取。 ●儲存媒體遺失。

二、現況分析(III)—電子病歷及其資安商機

- 醫療業於資通訊科技投資：

年度 \ 層級		醫學中心	區域醫院	地區醫院
2008	金額	7,188萬	2,084萬	479萬
	年成長率	34%	14%	25%
2009		6%	1%	-1%

資料來源：資策會產業情報研究所(MIC)

- 病歷資訊安全日益受到重視：硬體設備投資增加
- 2009年醫院於資訊安全投資將增加28%

三、發展趨勢

(一)國際推動電子病歷情形

(二)國際醫療資訊安全與隱私權保護規範

(三)我國電子病歷發展計畫

(一)國際推動電子病歷情形

國名	美國	英國	加拿大		新加坡	韓國	澳洲	我國
專案名稱	ARRA-HIT	NPfIT	Health Infoway		iN2015	CiEHR		NHIP 智慧醫療
期程	2011-2015 (5年)	2000-2010 (10年)	2001-2010 (10年)	-2015	-2015	2006-2013 (8年)	2009 2010 2012-2013	2008-2010 2009-2011
目標	鼓勵醫師及醫院採用電子病歷與其他健康資訊技術	建置整合式的IT基礎架構與系統，可以安全及有效地傳輸健康照護資訊	50%國民能擁有跨院際整合之電子病歷	100%國民能擁有電子病歷	建置跨院際整合之全國電子健康紀錄系統	任何時間地點均可以安全地使用電子病歷和決策資源以改善健康照護品質、安全及效率	跨院際且安全的交換個人健康紀錄	80%醫院實施電子病歷及60%醫院可院際病歷交換
投資金額	172億美元(約5,676億台幣)	62億英鎊(約3,286億台幣)	12億加幣(約360億台幣)		3億美元(約99億台幣)	預估2010年共投資11億美元(政府投資4.57億，民間投資6.2億)(約363億台幣)	5,700萬美元、5,150萬美元、2,700萬美元(約44.55億台幣)	2010年編列9.37億台幣(未編預算為53.91億台幣)

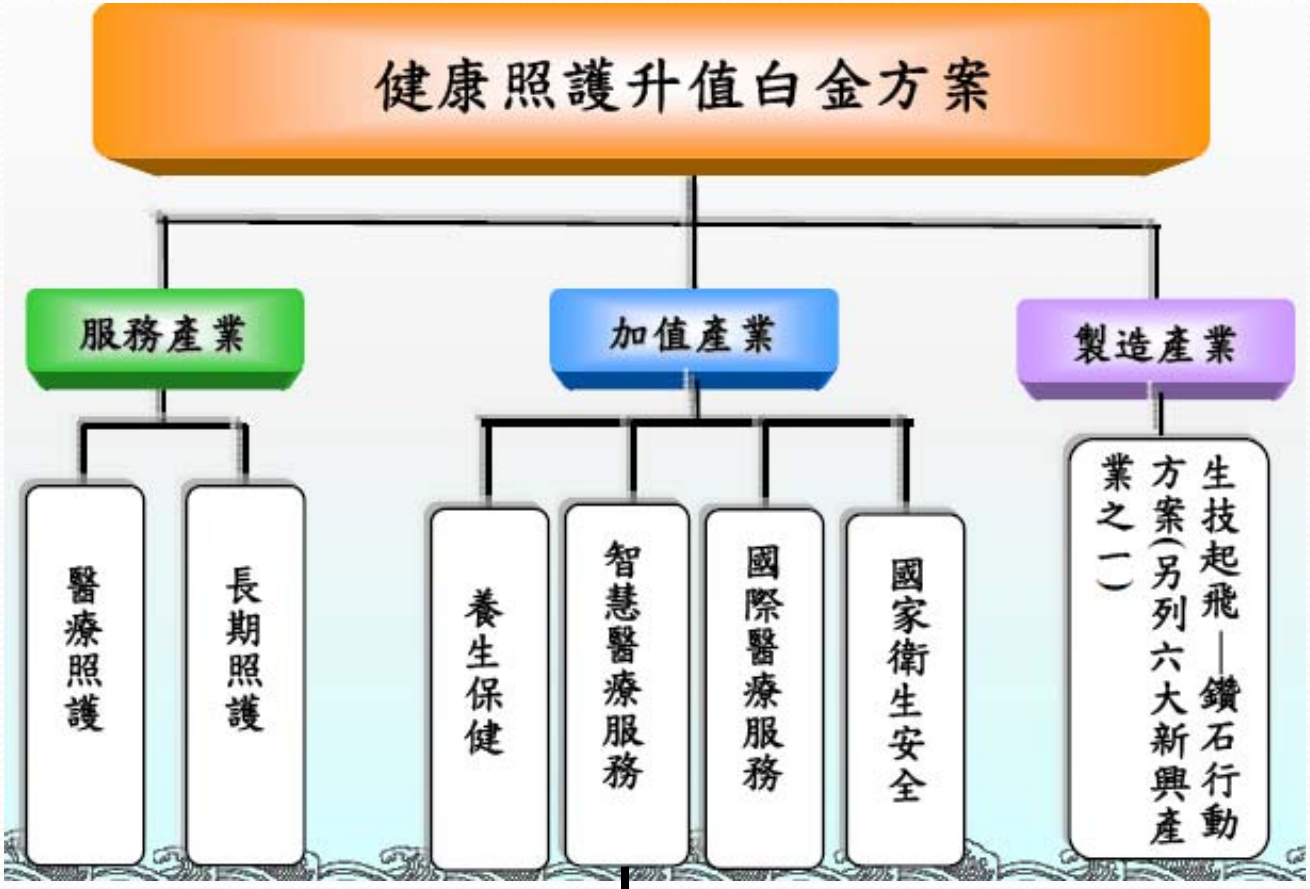
(二)國際醫療資訊安全與隱私權保護規範

國名	美國	澳洲
法規名稱	1. Health Insurance Portability and Accountability Act (HIPAA) (1996) • Security Rule(2003) • Standard for Privacy of Individually Identifiable Health Information (2002)	1. Privacy Act (1988) 2. The Privacy Amendment (Private Sector) Act (2000) 3. Guidelines on Privacy in the Private Health Sector (2001) 4. Guideline under Section 95 of the Privacy Act (1988) 5. Draft National Health Privacy Code (2002)

(二)國際醫療資訊安全與隱私權保護規範-續

國名	加拿大	紐西蘭	我國
法規名稱	1. Privacy Act (1983) 2. Personal Information Protection and Electronic Documents Act (2000)	1. Privacy Act (1993) 2. Health Information Privacy Code (1994)	1.電腦處理個人資料保護法 2.刑法第316條 3.醫師法第23條 4.護理人員法第27條 5.醫療法第49條 6.大法官會議解釋603號

(三)我國電子病歷發展計畫與「健康照護升值白金方案」之關聯



(三)我國電子病歷發展計畫－智慧醫療服務

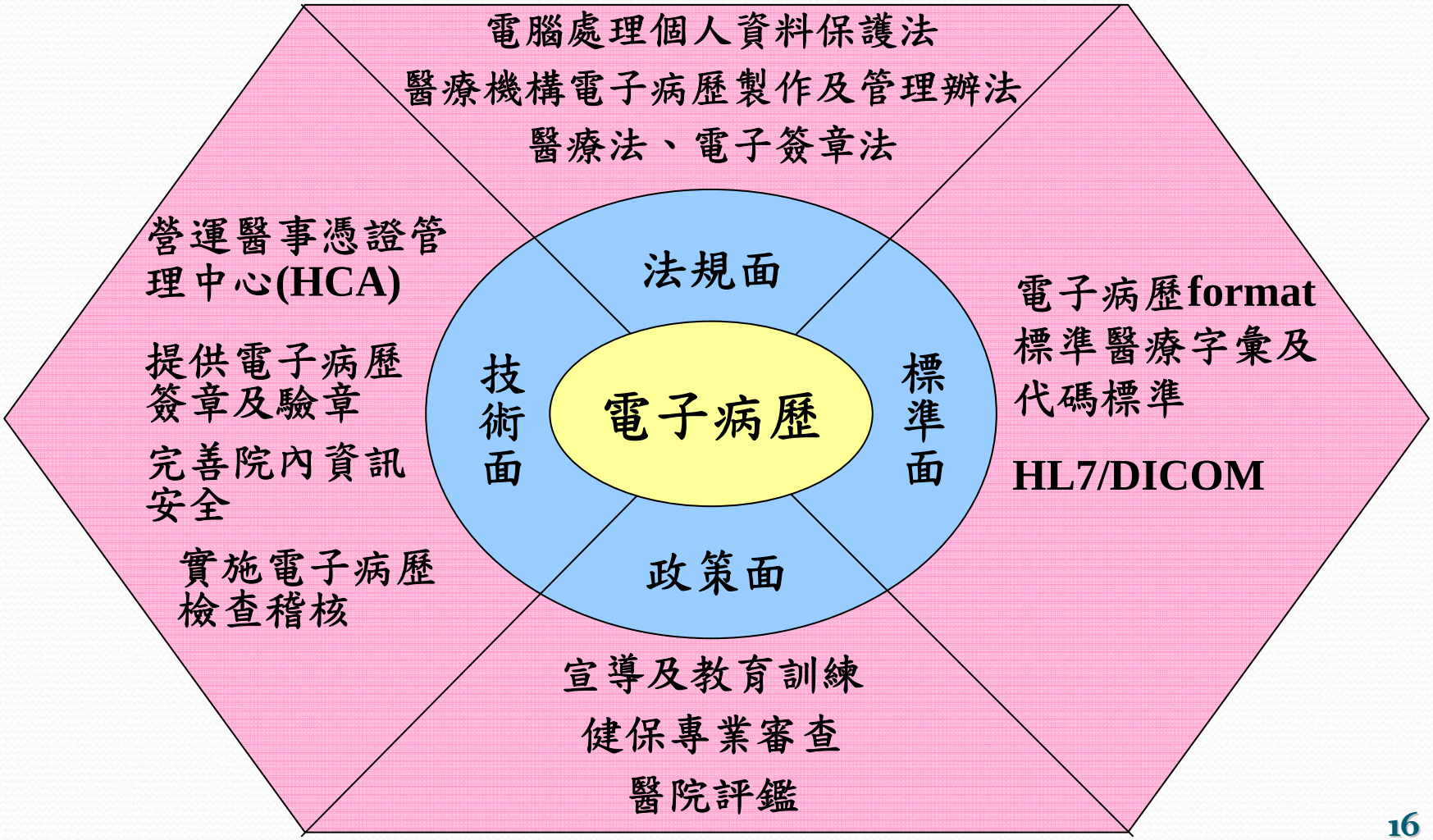
- 目標
  - 三年內(101年)推動全國80%醫院(400家)實施醫學影像及報告、檢驗檢查報告及用藥紀錄之電子病歷並至少60%醫院可院際互通。
  - 五年內(103年)達成醫療院所全面實施電子病歷及病歷交換系統。

(三)我國電子病歷發展計畫－智慧醫療服務經費需求

(單位：仟元)

工作項目	99	100	101	合計
1 建立我國電子病歷發展規範及基礎建設	99,000	93,000	68,000	270,000
2 落實醫院資訊發展與醫院評 鑑及健保審查作業結合	5,000	4,000	2,000	11,000
3 鼓勵及輔導醫療院所發展醫療作業資訊化及病歷電子化	596,000	2,513,500	2,559,500	5,669,000
4 推動院際電子病歷互通	0	30,000	70,000	100,000
合計	700,000	2,640,500	2,699,500	6,040,000

四、具體策略-電子病歷四大面向策略



四、具體策略

由技術面、法規面、政策面及標準面解決電子病歷資訊安全相關課題

技術面	●提供身份鑑別、時戳及加密功能 ●提供雙重身份認證之機制 ●提升資訊安全水準
法規面	●修法強化電子病歷安全及隱私保護 ●明定電子病歷應符合之資訊安全法規，並隨技術發展適時修正
政策面	●實施電子病歷檢查稽核 ●提供醫病雙方辨識之標記 ●以醫院評鑑及健保審查提供誘因 ●資安人才培訓
標準面	●制定電子病歷單張範本 ●建置電子病歷標準維護機制與管理系統

五、行動方案

技術面	●提供身份鑑別、時戳及加密功能 ●提供雙重身份認證之機制 ●提升資訊安全水準	1.擴大醫事憑證 (HCA憑證) 之應用 2.建立雙重身份認證之電子病歷交換中心 3.鼓勵醫院通過資訊安全管理系統之認證
法規面	●修法強化電子病歷安全及隱私保護 ●明定電子病歷應符合之資訊安全法規，並隨技術發展適時修正	1.持續修正醫療機構電子病歷製作及管理辦法 2.研議訂定我國電子病歷隱私保護法規
政策面	●實施電子病歷檢查稽核 ●提供醫病雙方辨識之標記 ●以醫院評鑑及健保審查提供誘因 ●資安人才培訓	1.研擬醫療機構電子病歷檢查機制 2.營運電子病歷驗證中心，頒授驗證標章 3.新制醫院評鑑基準加入資訊管理 4.培訓醫院資訊安全種子人員
標準面	●制定電子病歷單張範本 ●建置電子病歷標準管理系統與維護機制	1.制定電子病歷互通單張欄位標準 2.建立電子病歷標準管理系統，並透過維護機制保持單張版本一致

五、行動方案-技術面

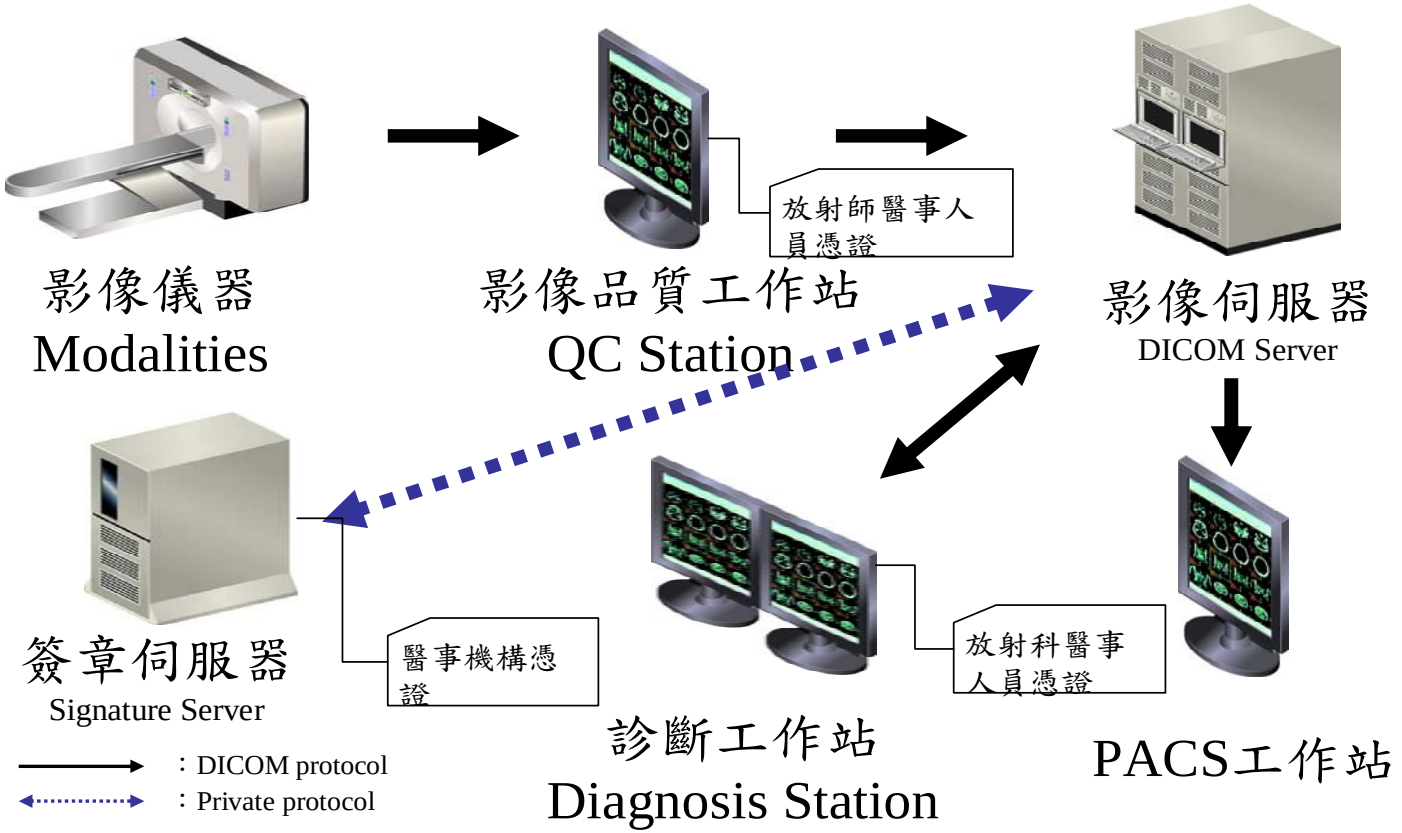
(一)擴大醫事憑證(HCA憑證)之應用

鼓勵及輔導醫院實施電子病歷

- 依法令病歷須以簽名或蓋章處，得以透過憑證提供之電子簽章為之，可確認簽署人的身份。
- 透過憑證加密來強化電子病歷安全，並保障病人隱私及病歷之完整性，有權限者透過憑證之解密功能，方可讀取病歷內容。
- 透過時戳作為送收電子病歷之時間證明，強化送收之不可否認性。

KPI	全國醫院實施電子病歷比例：2010年20 %(約100家)、2011年50 %(約250家)、2012年80 %(約400家)

HCA應用於醫療影像傳輸系統



五、行動方案-技術面

(二)建立雙重身份認證之電子病歷交換中心

- 建置電子病歷交換中心
  - 電子病歷分散式儲存在各醫院
  - 交換中心提供索引集中查詢
  - 醫院透過交換中心傳輸被查詢之病人病歷
  - 雙重身份認證(病人之健保IC卡＋醫事人員憑證IC卡)確保隱私及授權

KPI	2009年：建置影像交換中心 2010年：擴大影像交換中心為電子病歷交換中心，29家署立醫院透過此中心交換病歷

五、行動方案-技術面

(三)鼓勵醫院通過資訊安全管理系統之認證

- 輔導及補助醫院通過ISO 27001：2005資訊安全管理系統之認證，以達到公認之資訊安全水準，確保病歷資料安全，並維護民眾隱私及權益。

KPI	自2009年起每年輔導9％之醫院通過ISO27001資安認證，並逐年確實執行

五、行動方案-法規面

(一)持續修正「醫療機構電子病歷製作及管理辦法」

- 2004年4月28日修法通過，增訂醫療法第69條，賦予電子病歷法律地位。
- 2005年11月24日發布「醫療機構電子病歷製作及管理辦法」，符合本辦法者，不需印出紙本病歷。
- 此辦法是我國醫療機構實施電子病歷必須遵循之唯一規範，用意在於由醫療院所自主管理及持續改善其電子病歷。

五、行動方案-法規面

(一)持續修正「醫療機構電子病歷製作及管理辦法」-續

- **第3條**律定病歷資訊系統之建置，應符合資訊安全之規範。
- **第6條**規定電子病歷之簽章，應憑中央主管機關核發之醫事憑證為之。
- **第7條**規定醫療機構實施電子病歷，應將開始實施之日期及範圍報請直轄市、縣（市）主管機關備查，並應揭示於機構內明顯處所。

五、行動方案-法規面

(二)研議訂定我國電子病歷隱私保護法規

- 我國法律雖然少用隱私權，但法律規定中有關名譽、信用、秘密等保護，與保護隱私權之精神近似。
- 未來比照美國HIPAA（美國健康醫療保險可攜與責任法案）研擬我國是否對醫療資訊隱私權律定集中立法。

五、行動方案-政策面

(一)研擬醫療機構電子病歷檢查機制

- 依據醫療法第26條 (醫療機構應接受主管機關對其病歷檢查)規定辦理。
- 採用ISO 27001的PDCA精神，依據「醫療機構電子病歷製作及管理辦法」制定查核項目。
- 對宣告實施電子病歷之醫院採不定期及事後檢查，敦促其持續改善。

KPI	2009年將完成醫療機構電子病歷檢查機制之研擬

五、行動方案-政策面

(二) 營運電子病歷驗證中心，授予驗證標章

- 驗證醫療機構之電子病歷是否符合「醫療機構電子病歷製作及管理辦法」規定。
- 提供電子病歷驗證標章供民眾辨識，並增加醫院之競爭力。
  - 設立全國電子病歷驗證網站。
  - 設計驗證標章，並宣導其意義及榮譽。
  - 提供醫療院所電子病歷驗證(含複驗)服務。
  - 培訓電子病歷驗證人力並提供諮詢服務。

KPI	2010年開始營運電子病歷驗證中心

五、行動方案-政策面

(三)新制醫院評鑑基準加入資訊管理

- 為建立安全、以病人為中心的醫療服務體制，衛生署自1988年起開始辦理全國醫院評鑑，2007年起全面實行新制醫院評鑑。
- **新制**增訂「資訊管理」之評鑑項目：要求醫院應有完善之資訊管理機能，確保資訊具有保密性、安全性、可用性與完整性等必備條件。
- 依評鑑結果搭配相對之評鑑加分機制，可提供醫療院所持續實施電子病歷之強制力及誘因。

五、行動方案-政策面

(四)培訓醫院資訊安全種子人員

- 建立醫事人員資安意識，降低人為作業疏失機率。
- 培訓醫院資訊安全種子人員，並取得ISO 27001主導稽核員資格，以協助醫院建立資訊安全管理系統。
- 辦理醫院資訊安全講習，提升醫院內部人員資訊安全及隱私保護的意識及能力。

KPI	每年持續提供每家醫院一名ISO 27001主導稽核員訓練名額，並辦理80場醫院講習

五、行動方案-標準面

(一)制定電子病歷互通單張欄位標準

- 依醫療院所院際病歷交換所需，訂定108張電子病歷單張欄位標準，並針對電子簽章欄位做規範。
- 未來將可依據病歷交換標準，規定傳輸之必要單張，提供適當的病歷內容，使病患隱私權受侵害之風險降低。

KPI	2009年將完成108張電子病歷單張欄位標準

五、行動方案-標準面

(二)建立電子病歷標準管理系統，並透過維護機制保持單張版本一致

- 建置電子病歷標準管理系統，電子病歷單張經確認或制定後，皆需於系統進行註冊以保持單張版本之一致性。
- 依循提案、起草、公告、審訂、投票及公布之6個步驟建立維護機制，確保國內電子病歷單張標準之完整性及正確性。

KPI	2009年建立電子病歷標準管理系統

六、討論題綱–議題一

案由：病人對其病歷內容之全部或部分的閱覽及傳遞交換，如何行使同意權並顧及資訊安全？

說明：近年來民眾對自己的醫療資訊隱私保障意識高漲，特別是有特殊疾病者(如：AIDS、精神病)、VIP病患或政治人物之病歷內容更要求保護隱私，一旦資料外洩，可能影響病人的就學、就業、就醫及居住之權益，更甚者導致國家、社會及政治動盪不安。

擬辦：醫療院所實施電子病歷可達無紙化及無片化，惟病人之各類同意書仍有困難，是否可由人手一張之健保IC卡提供病人電子簽章機制？並將醫事人員卡結合健保卡，以符「減卡」目標？

六、討論題綱-議題二

鑑於醫療資訊對人民隱私的敏感性以及其利用對人類福祉所生的助益，我國對於醫療資訊隱私與安全的保護，是否有仿效美國以及紐西蘭等國訂定專法加以規範的必要？

簡報完畢

敬請指教