衛 生 福 利 部
MINISTRY OF HEALTH AND WELFARE

112 年醫院評鑑及教學醫院評鑑說明會

醫療資訊安全政策

衛生福利部資訊處 王復中

2023/4/27

簡報大綱

01 政策方向

02 資安病安

03 法規規範

04 危機轉機

111年醫院評鑑及教學醫院評鑑說明會

本部資安目標與執行策略

整體目標：持續精進現有措施，使資安作業常規化、可預期，並擴大執行範圍

推廣 資安聯防平台

- 策略1 擴大招收HISAC會員
- 策略2 強化HISAC情資分享內容
- 策略3 擴大HSOC監控範圍

深化 情資交流與應變演練

- 策略1 情資座談會
- 策略2 辦理各項資安演練作業
- 策略3 資安長共識營

目標

落實 資安政策與法規遵循

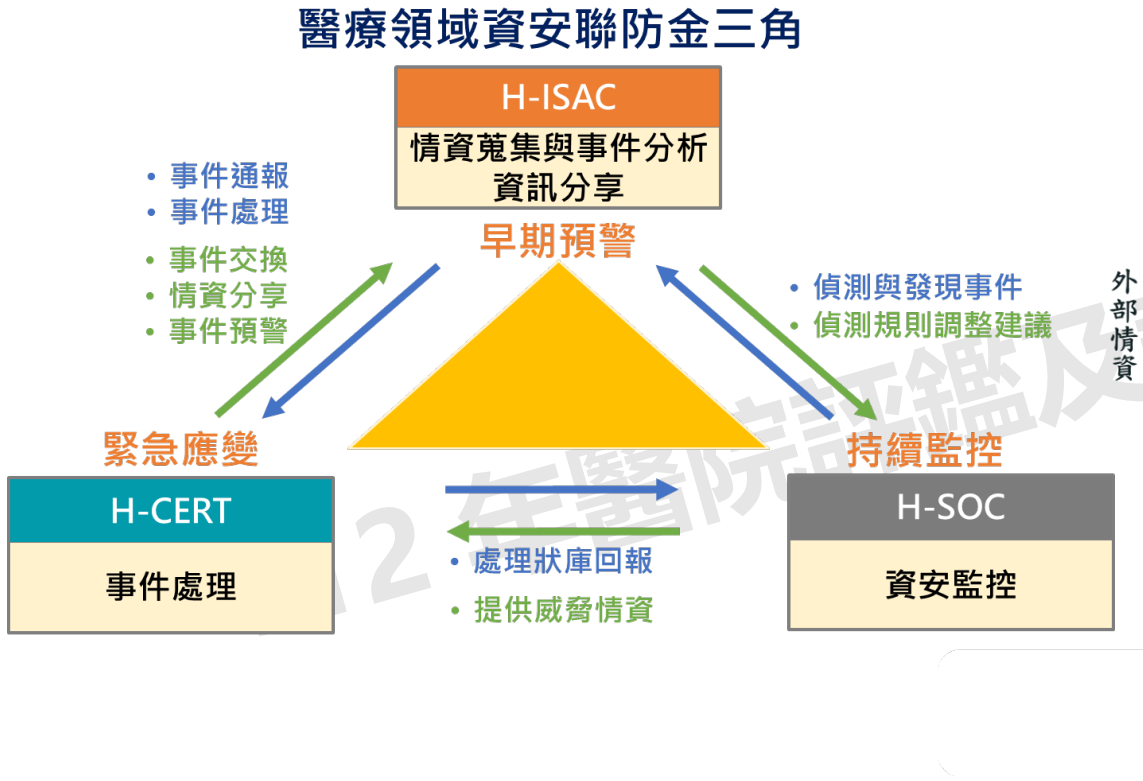
- 策略1 檢視資安維護計畫、實施情形
- 策略2 推動IT、OT資安防護基準
- 策略3 醫院評鑑、資安稽核

培育 醫療領域資安人才

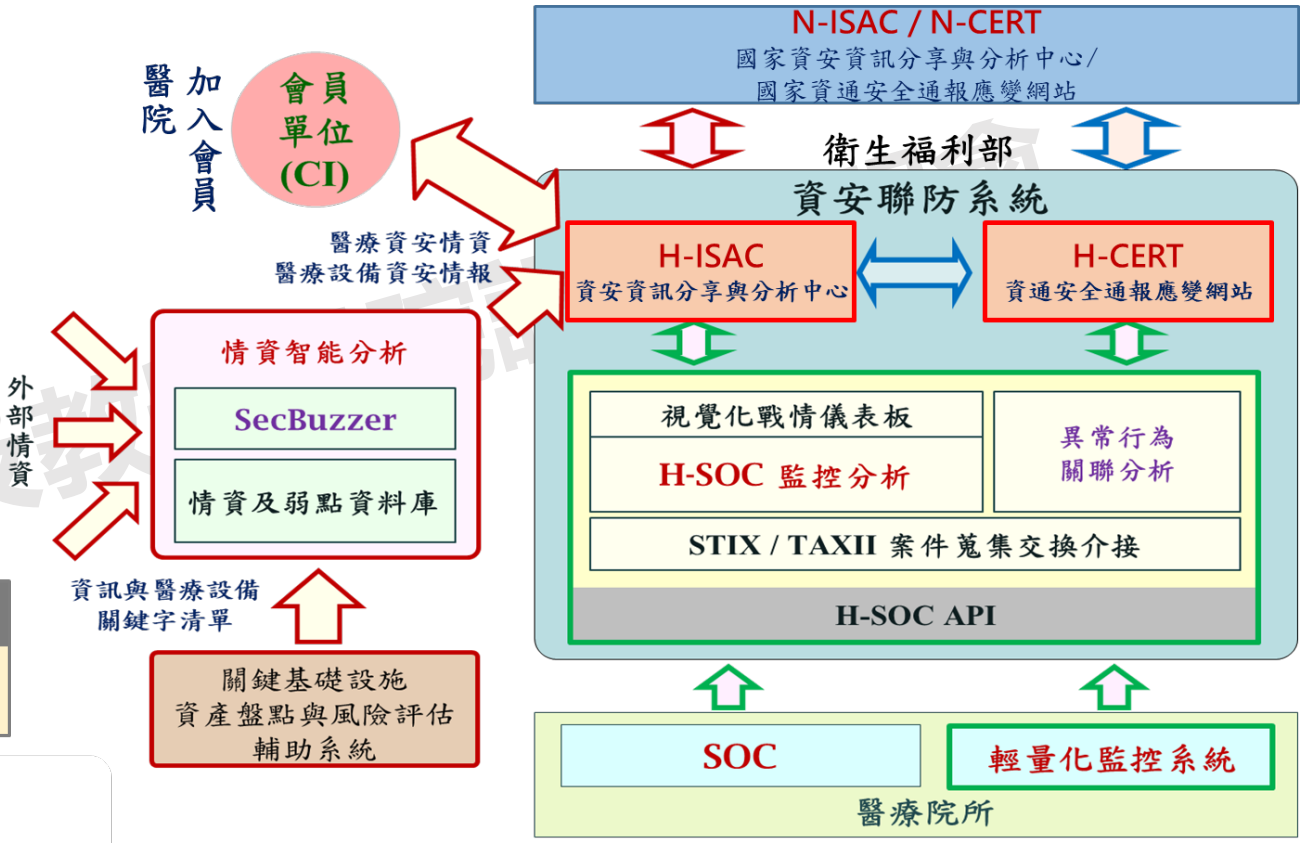
- 策略1 依領域藍圖培訓資安人才
- 策略2 建立資安人才資料庫
- 策略3 儲訓醫療領域稽核委員

資安聯防平台

聯防平台，建立雙向溝通管道



擴大參與，推動聯防廣邀H-ISAC會員



情資交流分享

H-ISAC平台會員服務

情資交流分享：公開資訊發布訊息

- 一般訊息、預警資訊
- 醫療資安、醫療設備資安新聞
- 勒索軟體因應情報、勒索軟體週報
- 釣魚信件攻擊因應策略
- 資安防護建議與程序
- 中繼站黑名單
- 資安事件分析報告
- 活動資訊、其他資安訊息

衛生福利部資安聯防系統：H-ISAC,H-CERT整合平台

每年進行會員警訊發布與通報演練

警訊發布

通知進行通報演練(提供演練情境)

警訊單資料

警訊編號	HISAC-MES-INT-2020-0022
發布時間	2020-09-29 11:31:13
警訊種類	入侵攻擊情報
事件類型	系統被入侵
警訊來源	H-ISAC
外部發布編號	
警訊發現日期	2020-09-29
警訊主旨	(演練)醫療院所門診區電腦發現遭勒索軟體攻擊，請會員機構應啟動醫院內部通報流程，並於1小時內進行事件通報。
事件描述	近期各醫療院所門診相關電腦遭受勒索軟體攻擊，導致門診電腦檔案遭加密，中斷達30分鐘以上。事件描述請參考附件。 請會員醫療機構應依發生資安事件之情境於1小時內進行事件通報，並啟動醫院內部通報流程，進行事件等級、影響範圍、損害程度、因應措施之評估，依法定時限內完成復原或完成損害管制。 備註：會員進行通報單處理之Step5與Step6(需外部支援)，請務必點選「確定支援廠商」按鈕，請勿自行填完送出。
建議措施	1.應保留證據，並至H-ISAC系統平台進行資安事件通報應變處理程序。 2.將加密勒索訊息視窗與已加密資料夾檔名予以拍照截圖存證。 3.立即中斷電腦網路連線，避免災情擴大。 4.立即強制電腦關機，不讓勒索病毒繼續加密電腦中的檔案。 5.通知機關資訊人員或廠商協助搶救還沒被加密的檔案。 6.建議重新安裝作業系統與應用程式，並安裝最新修補程式。 7.備份資料復原前，應以防毒軟體檢查，確保沒有殘留的惡意程式。 8.加強教育訓練宣導，通知所有同仁有狀況立即回報。
參考資料	
手法研判	
是否需回覆	否
發布時是否同時簡訊通知	是
簡訊內容	H-ISAC資安警訊警訊編號(演練)已寄至貴單位連絡人信箱，請於1小時內進行事件通報與處理程序。 網站連結 https://hisac.nat.gov.tw/ ，客服電話0809070166
是否為演練	是

附加檔案

附件名稱	附件說明	附件大小	驗證碼(SHA256)
資安事件通報演練情境.pdf		382.2 KB	4f0893850f193cc0bb1de2154d4b55e09708d301e48b456f726a65de98d06981

通報演練

收到警訊通知之會員機構，依照演練情境進行通報作業

Step1.事件資料 | Step2.事件分類 | Step3.影響等級 | Step4.評估支援 | Step5.緊急應變 | Step6.結案作業

Step 2. 詳述事件發生過程

二、事件發生過程

事件發生時間	2020-09-29 13:45:37
事件分類與異常狀況	○ 網頁攻擊 ○ 非法入侵 ○ 阻斷服務(DoS/DDoS) ○ 設備異常 ◉ 其他 異常原因 勒索軟體攻擊
事件說明及影響範圍	(演練)醫療院所門診區電腦發現遭勒索軟體攻擊，請會員機構應啟動醫院內部通報流程，並於1小時內進行事件通報。
是否影響其他政府機關(構)或重要民生設施運作	否
事件通報來源	○ 自行發現 ◉ 警訊通知 警訊發布編號 HISAC-MES-INT-2020-0022

透過定期通報演練作業，確保醫院熟悉操作並時限內通報

Step1.事件資料 | Step2.事件分類 | Step3.影響等級 | Step4.評估支援 | Step5.緊急應變 | Step6.結案作業

Step 5. 緊急應變措施(其他)

五、完成損害控制或復原

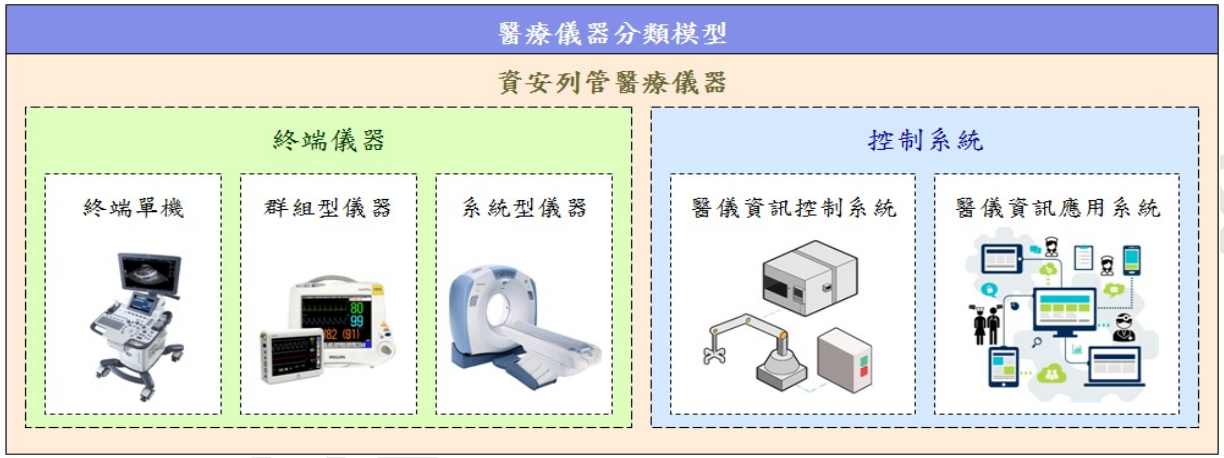
保留受害期間之相關設備紀錄資料	☑ 已保存遭入侵主機事件檢視器 ( ) ☑ 已保存防火牆紀錄 ( ) ☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共0個 ☐ 其他保留資料或處置說明，【如未保存資料亦請說明】
事件分析與影響評估	☑ 異常連線行為【請列出異常IP與異常連線原因，如：存取後台管理頁面】1.1.1.1 ☐ 異常帳號使用【請列出帳號並說明權限，與判別準則，如：非上班時間帳號異常登入/登出】 ☐ 發現資料外洩情況 ☐ 影響評估說明補充【請填寫補充說明】
封鎖、根除及復原	☐ 移除未授權存在之惡意網頁/留言/檔案/程式，共0筆【請說明程式名稱或路徑、檔名】 ☑ 將可疑IP/Domain Name列入阻擋清單【請說明設定阻檔之資訊備與阻檔之IP/Domain Name】 1.1.1.1 ☐ 停用/刪除異常帳號【請說明停用/刪除之帳號】 ☐ 中斷受害主機網路連線行為至無安全性疑慮 ☑ 重新建置作業系統與環境，完成日期2020-09-29 ☑ 惡意程式樣本送交防毒軟體廠商，共1個 ☐ 應變措施補充說明【請填寫補充說明】
應變處置說明	損害控制或復原之執行狀況 已完成全部系統之復原 ◉ 已完成損害控制，未有擴大損害情形 ○ 已完成損害控制並復原，恢復資安事件造成的損害 完成損害控制或復原時間2020-09-29 00:00:00
是否需要支援	是
期望廠商支援內容與提供廠商之事件描述	確定支援廠商支援勒索軟體
支援廠商	數聯資安股份有限公司

近期推動資安重點議題

醫療儀器資通系統防護基準(CI)

醫療儀器分類、分級

- 將醫療儀器分為2群、5類
- 再依機密性、完整性、可用性分為普、中、高三級
- 針對醫療儀器設備分類及等級訂定防護基準，並納入後續稽核項目



醫院評鑑基準及評量項目增加資安事項

國家層級資通安全風險評估(CI)

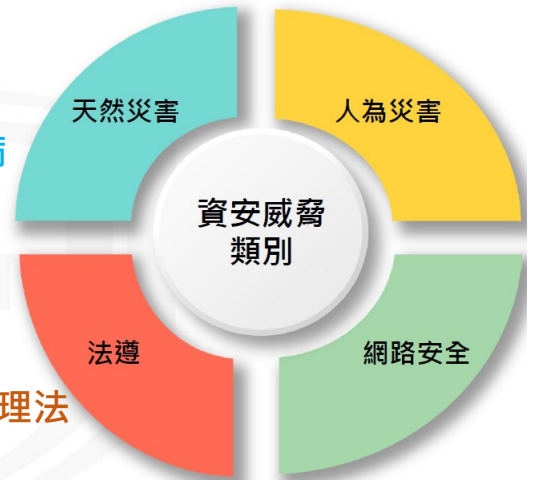
配合行政院完成逐年完成資安風險地圖

- 111年各領域導入3個CI、112年導入6個、113年完全導入，並完成我國資安風險地圖

評估流程

- 列出可能之資安威脅項目
- 撰寫資安風險情境(應包含攻擊方式或災害描述、受攻擊目標、受影響範圍及項目等)
- 依照情境發生之可能性及衝擊進行評估

1.地震
2.風災
3.水災
4.法定傳染病



1.委外廠商故意/意外
2.內部人員故意/意外
3.外部人員惡意破壞
4.相依CI供應失效
5.維運不當

1.資通安全管理法
2.電信法規
3.傳播法規

1.釣魚郵件
2.DDoS攻擊
3.勒索軟體
4.APT攻擊
5.劫持事件

醫療三大法律規範

機構與人的管理規範

一、醫事機構（業務）

管理法規 以醫療機構、醫療業務之管理，病人 權利之保護，及均衡醫療資源等為規範內容。

二、醫事人員管理法

以醫事人員之資格、執業、業務與義務、公會組織等為規範內容。)

個人資料保護法之目的

一、避免人格權受侵害

二、促進個人資料合理利用

資通安全法之目的

為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益

112 年醫院評鑑

「醫療機構電子病歷製作及管理辦法」修法沿革

94年11月24日
- 發布訂定全文 7 條

97年12月25日
- 發布修正全文 8 條
- 增訂保持病歷資訊系統時間正確性之機制

98年8月11日
- 發布修正全文 8 條
- 增訂電子簽章、醫事憑證等規定，並推動無紙化

111年7月18日
- 發布修正全文23條
- 強化電子病歷資通安全，訂定病歷交換標準格式法源

111年12月7日
- 公告鬆綁醫療法人投資限制

112年醫院評鑑

Hardware Domain

System Integration Domain

Vendor Regulated

Before 1990 | 1990 - 2022 | Since 2022

醫療機構電子病歷製作及管理辦法修正案(1/3)

新增條文	說明
第六條 第三條第一項系統，醫療機構得委託大專校院、依法登記或立案之法人、機構或團體（以下併稱受託機構）建置及管理之，並由醫療機構負本法及本辦法規定之責任。 前項醫療機構之委託，應訂定書面契約。但有下列情形之一者，得免訂定書面契約： 一、委託所屬醫療法人或其他法人之其他附設醫院。 二、委託所屬學校之其他附設醫院。 三、委託所屬機關設立之其他醫院。前項受託機構，以大專校院及依法登記或立案之法人、機構或團體為限。 **第一項受託機構，應通過中央主管機關認可之資訊安全標準驗證，並有證明文件。**	**一、本條新增。** 二、基於資通系統及資訊安全之專業性，醫療機構得委託專業之大專校院及依法登記或立案之法人、機構或團體（以下簡稱受託機構）建置及管理系統；惟應考量受託機構之專業能力與經驗、委託項目之性質及資通安全需求選任之，以確保系統安全，爰為第一項規定。 三、病歷係為特種個人資料，無個人資料保護法第六條但書規定之情形者，不得蒐集、處理或利用；本法第七十二條亦明定，醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩漏。為免發生爭議，爰於第二項要求醫療機構委託受託機構建置及管理系統時，應訂定書面契約。惟醫療機構委託所屬醫療法人或其他法人、所屬學校之其他附設醫院或所屬機關設立之其他醫院建置系統者，如認為發生爭議時，可明確與受託機構區分責任歸屬（例如以口頭、文書或其他方式約定權責分工），得免訂定書面契約，爰以但書為例外之規定。 四、為讓醫療機構挑選適當之受託機構以確保品質，且目前國內有能力設置、管理電子病歷資訊系統之專業機構家數並不多（約十家以下），爰於第三項規範受託機構之資格條件為：應通過中央主管機關認可之資訊安全標準驗證（包含ISO/IEC 27001、ISO/IEC 15408或其他國際認定之資訊安全標準）。

醫療機構電子病歷製作及管理辦法修正案(2/3)

新增條文	說明
第八條 **醫療機構就系統資料之蒐集、處理與利用及資料庫之使用，運用雲端服務或委託受託機構提供雲端服務時，應依下列規定辦理：** 一、採取適當風險管控措施。 二、採取避免醫療業務中斷措施。 三、對雲端服務業者進行監督，並得視需要，委託受託機構或其他專業機構協助監督。 四、停止或終止雲端服務時，資料移轉回委託機構或其他雲端服務業者之機制。 前項雲端服務之資料儲存地點，應設置於我國境內。但因特殊情形，經中央主管機關核准者，不在此限。 **第一項提供雲端服務者，應通過中央主管機關認可之資訊安全標準驗證，並有證明文件。**	一、本條新增。 二、雲端服務（Cloud Service）係資訊時代下之必然產物，結合雲端運算（Cloud Computing）、雲端儲存（Cloud Storage）、網路連線，與商業需求之新時代網際網路服務之雲端服務是無可避免，爰於第一項明定醫療機構使用雲端服務之相關規定。 三、病歷係特種個人資料，爰於第二項規範雲端服務之資料儲存地點，以我國境內為原則；惟考量與國外合作等特殊情形，爰以但書規定例外情形。 四、為確保雲端服務之資訊安全，爰於第三項規範提供雲端服務者之條件，並授權中央主管機關另行公告認可之資訊安全標準驗證。

醫院評鑑及教學醫院評鑑說明會

醫療機構電子病歷製作及管理辦法修正(3/3)

條文	公告之資訊安全標準		說明
第6條第3項 第一項受託機構，應通過中央主管機關認可之資訊安全標準驗證，並有證明文件。	資安管理	ISO/CNS 27001	● 驗證範圍應涵蓋專案開發、支援、實作、維護、管理或操作等相關流程之一，驗證文件應持續有效，且發證單位應為國際認證論壇(International Accreditation Forum，IAF)認證機構認可之驗證機構。
	個資保護	ISO/CNS 27701：自公告日起3年內增列	
第8條第3項 第一項提供雲端服務者，應通過中央主管機關認可之資訊安全標準驗證，並有證明文件。	資安管理	ISO/CNS 27001	● 本辦法第八條第三項所定提供雲端服務者，不得為行政院公共工程委員會101年09月13日工程企字第10100346580號函所定陸資廠商 ● 驗證範圍應涵蓋所使用之雲端服務相關流程，驗證文件應持續有效，且驗證文件之發證單位應為國際認證論壇(International Accreditation Forum，IAF)認證機構認可之驗證機構。
	個資保護	ISO/CNS 27701（或BS10012）	
	雲端安全及個資	ISO/CNS27017 ISO/CNS27018	
	持續營運	ISO/CNS 22301：自公告日起3年內增列	

醫院評鑑及教學醫院評鑑說明會

個資保護：醫院安全維護計畫

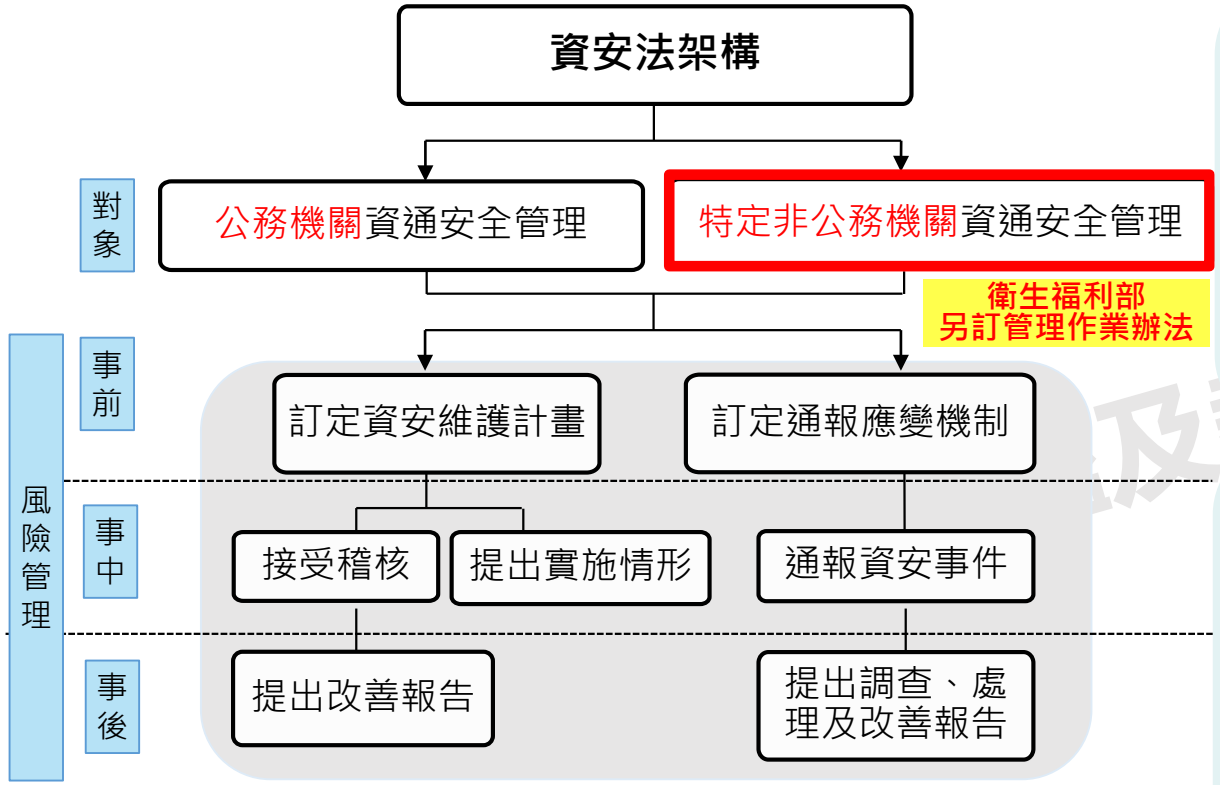
醫院個人資料檔案安全維護計畫實施辦法(適用總床數達一百床以上)

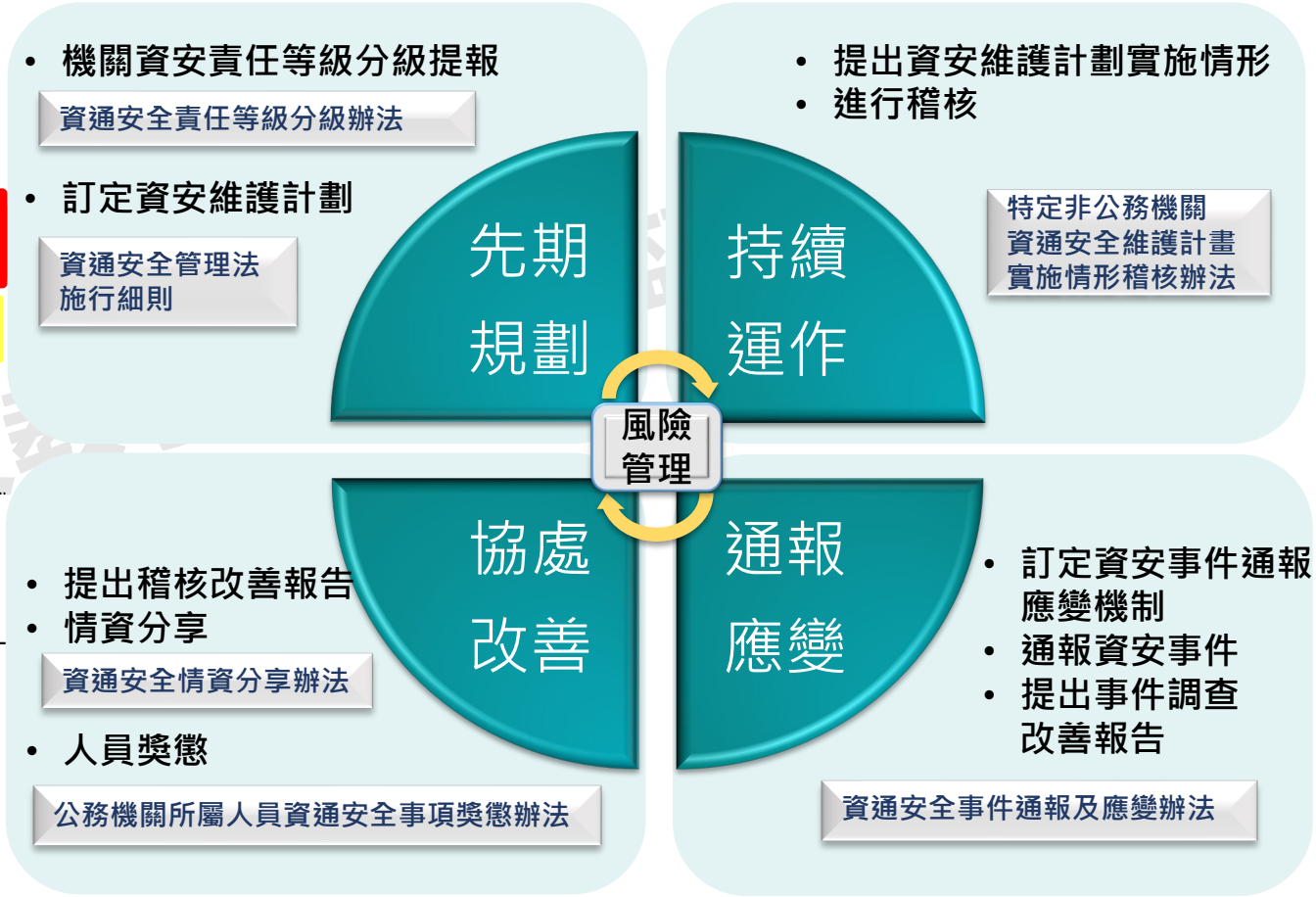
一、本辦法適用範圍。（§2）
二、本辦法所稱主管機關：在中央為衛生福利部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。（§3）
三、本辦法用詞，醫院、所屬人員、專責人員與查核人員之定義。（§4）
其中醫院是指總床數達一百床以上之私立醫院、醫療法人醫院及其他法人附設醫院。專責人員與查核人員不得為同一人
四、醫院應依本辦法規定訂定安全維護計畫，明訂應載明之事項。依醫院業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討或修正安全維護措施（§5, §6）
五、醫院訂定管理程序及個人資料範圍及項目應確認其必要性，有非屬特定目的必要範圍或特定目的消失，應適當處置。（§7）
六、醫院於蒐集個人資料時，應符合所定之類別及範圍。傳輸個人資料時，應採取必要保護措施。（§8）
七、醫院蒐集個人資料依規定告知。（§9）
八、醫院委託他人蒐集、處理或利用個人資料於委託契約或相關文件中，明確約定內容。（§10）
九、醫院對其所屬人員採取之措施，並使所屬人員明瞭個人資料保護相關法令規定、責任範圍、作業程序。（§11 ,§12 ）
十、醫院對所持有之個人資料檔案，應設置必要之安全設備及防護措施事項列項。（§13, §13-1 ）
十一、於發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害事故時迅速處理之事項。（§14）
其中明訂於發現事故時起七十二小時內，以書面通報直轄市、縣（市）主管機關及副知中央主管機關，並公告通報紀錄格式與季通報紀錄格式。
十二、醫院留存相關之證據資料與期限規定。（§15）
十三、醫院業務終止後，規定製作紀錄之方式。（§16）
十四、醫院應檢視所定安全維護計畫之合宜性，必要時應予修正。（§17）
十五、查核人員應每年評核計畫執行情形及成效，評核結果向醫院提出報告，專責人員依評核結果檢討、修正。直轄市、縣（市）主管機關應定期查核。（§18）
十六、本辦法於公立醫院，準用之。（§19）

資通安全管理法規架構

適用對象：公務機關與及特定非公務機關(經指定程序行政院核定者)

(母法及六子法)

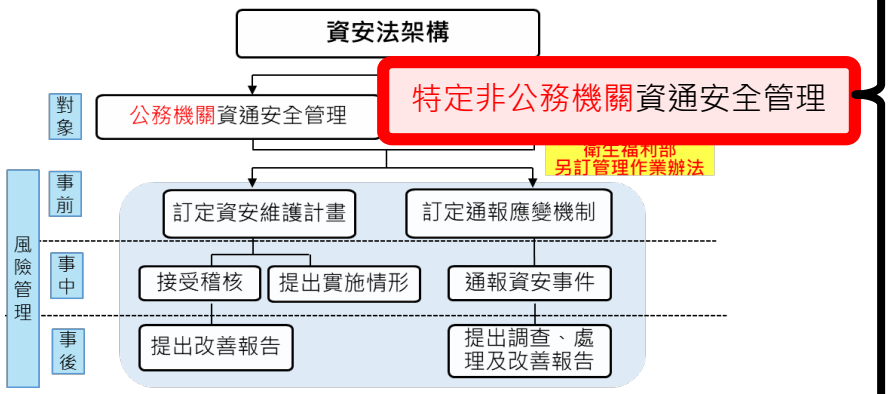




資料來源：數位部資安署

資通安全管理：安全維護計畫

衛生福利部訂定「所管特定非公務機關資通安全管理作業辦法」



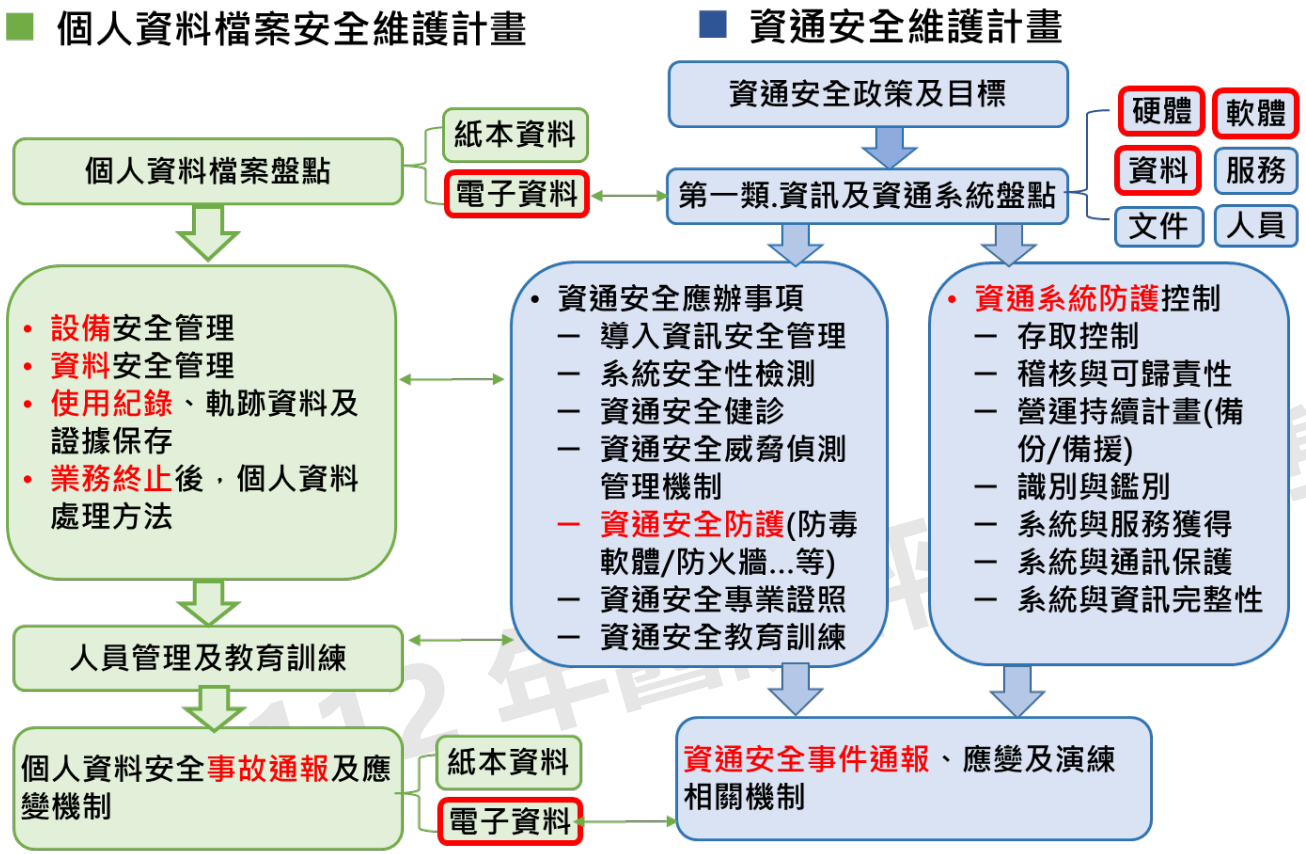
一、本辦法所稱關鍵基礎設施提供者之定義。（§2）
二、衛生福利部所管特定非公務機關資通安全維護計畫及實施情形之內容應載明事項。（§3）
三、衛生福利部所管特定非公務機關資通安全維護計畫提出方式。（§4）
四、衛生福利部所管特定非公務機關資通安全維護計畫實施情形提出方式。（§5）
五、稽核之頻率、內容與方法及其他相關事項。（§6）
六、稽核之通知及期程調整規定。（§7）
七、受稽核者之配合事項。（§8）
八、稽核小組之組成及利益迴避與保密義務之規定。（§9）
九、稽核結果報告之內容及交付時程。（§10）
十、改善報告之提出方式及時程。（§11）
十一、本辦法之書面得以電子文件為之。（§12）

提交資通安全維護計畫內含事項規定

- 依《資通安全管理法施行細則》第6條規定，應包含：
  - 一、核心業務及其重要性。
  - 二、資通安全政策及目標。
  - 三、資通安全推動組織。
  - 四、專責人力及經費之配置。
  - 五、公務機關資通安全長之配置。
  - 六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。
  - 七、資通安全風險評估。
  - 八、資通安全防護及控制措施。
  - 九、資通安全事件通報、應變及演練相關機制。
  - 十、資通安全情資之評估及因應機制。
  - 十一、資通系統或服務委外辦理之管理措施。
  - 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。
  - 十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

資安與個資保護管理融合議題

醫院二項安全維護計畫適度管理融合



醫院二項事件通報作業適度管理融合

相關通報規定

- 個人資料安全事故通報及應變：
  - 電子資料發生個人資料被竊取、洩漏、竄改或其他侵害事故，亦為資安事件。
  - 個資事件於發現事故時起七十二小時內，以書面通報直轄市、縣（市）主管機關及副知中央主管機關。(依「醫院個人資料檔案安全維護計畫實施辦法」第14條)
  - 資安事件應於知悉1小時內通報立案，通報方式為登入衛福部H-ISAC平台網頁完成通報立案及時限內應變處理結案。
  - 通報人員不同應建立資訊互通機制。

資通安全管理：稽核作業

管理作業辦法：執行所管特定非公務機關稽核作業

- **稽核對象**：衛生福利部所管特定非公務機關
- **稽核方式**：技術檢測一天及實地稽核一天

稽核作業重點

- **資通安全維護計畫內含事項**
- **資通安全責任等級分級辦法第11條附表規定應辦事項：**

  以資安責任等級 A級機關應辦事項為例

  - 資通系統分級及防護基準：針對自行或委外開發之資通系統，依附表九完成資通系統分級。
  - **全部核心資通系統** 2年內完成ISMS之導入，3年內完成驗證。
  - 配置**4名**資通安全**專責**人員 (A級4名, B級**2名**,C級**1名**)
  - 資通安全威脅偵測機制建置：依規定時限完成威脅偵測機制建置，並持續維運。
  - 資安教育訓練要求，分資安專責人員、資安專職人員以外之資訊人員與一般使用者及主管三類，受訓符合規定。

- **衛生福利部發佈納入管理要求，機關應明訂納入維護計畫執行 (H-ISAC公告)**

資通安全管理：通報應變

資通安全事件通報及應變辦法

- 依據資安事件通報應變辦法第4條規定：
  公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。
- 依據資安事件通報應變辦法第11條規定：
  特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。

規範對象

註:醫療中央目的業主管機關為衛生福利部。

公務機關

- **中央、地方機關(構)**
- **公法人**

特定非公務機關

- **關鍵基礎設施提供者**
- **公營事業**
- **政府捐助之財團法人**

資安法規定軍事機關、情報機關由上級機關另訂管理辦法。

資安事件通報應變管理程序

- 本辦法明定機關應設置內部「資安事件通報作業」與「資安事件應變作業」規範 (公務機關第2章第9條與第10條, 特定非公務機關第3章第15條與第16條

項目	資安事件通報作業	資安事件應變作業
目的	知悉資安事件發生時，迅速依作業規範執行通報作業，並確保相關人員熟悉作業流程	發生資安事件時，可依作業規範保留必要事件紀錄，防止災情擴大，並釐清事件發生經過
規範事項	✓ 判定事件等級之流程及權責 ✓ 事件之影響範圍、損害程度及機關因應能力之評估 ✓ 資通安全事件之內部通報流程 ✓ 通知受資通安全事件影響之其他機關之方式 ✓ 前四款事項之演練 ✓ 資通安全事件通報窗口及聯繫方式 ✓ 其他資通安全事件通報相關事項	✓ 應變小組之組織 ✓ 事件發生前之演練作業 ✓ 事件發生時之損害控制機制 ✓ 事件發生後之復原、鑑識、調查及改善機制 ✓ 事件相關紀錄之保全 ✓ 其他資通安全事件應變相關事項

行政院國家安全會報訂定「資通安全事件通報應變管理程序(範本)」

衛生福利部訂定「所管特定非公務機關關鍵基礎設施提供者—資通安全維護計畫(範本)」
(含資通安全事件通報、應變及演練機制規範)

衛生福利部資安防護規範與醫院評鑑

政策作為	強度要求	CI醫院/公務機關	非CI醫院	基層診所
● 基層醫療院所資安防護參考指引(註)	普	-	V • 未申請評鑑醫院	V
● 醫院評鑑基準之資安防護與其管理措施條文 ● 資通安全管理法及其子法 ● 衛生福利部醫療領域資通系統資安防護基準(草案) ● 基層醫療院所資安防護參考指引(註)	中	-	V • 符合評鑑 • 參考法規 • 參考規範 • 參考規範	
● 資通安全管理法及其子法 ● 衛生福利部所管特定非公務機關資通安全管理作業辦法 ● 衛生福利部醫療領域資通系統資安防護基準(草案) ● 醫院評鑑基準之資安防護與其管理措施條文	高	V • 符合法規 • 符合法規 • 符合法規 • 符合評鑑		

註: 衛生福利部 110年7月21日公告「基層醫療院所資安防護參考指引」，適用對象為資通安全管理法未納管之區域醫院及地區醫院、一般診所。

醫學中心醫院評鑑基準及評量項目(1/4)

醫學中心 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112 年度醫院評鑑基準及評量項目(醫學中心適用)		
條號	條文	評量項目
1.4.8	資訊部門配合臨床及行政部門建立完善作業系統，且院內各系統連線作業及院外聯繫系統功能良好	**優良項目：** 4. 設有資訊安全管理委員會或相關組織，負責資訊安全工作推動及追蹤，並由現任副院長以上層級人員擔任資通安全長，訂有資訊安全管理計畫且召開跨部門之管理會議，能針對資安列管設備(含醫療儀器及其他支援設施)、臨床與行政決策系統進行討論，落實資訊安全以確保病人安全及提升醫療品質。(原1.5.8-優良4修) **評量方法及建議佐證資料：** 3.資訊安全管理委員會或相關組織之章程與會議紀錄。(符合) 7.資訊安全管理年度計畫。(優良)

醫學醫院評鑑說明會

醫學中心醫院評鑑基準及評量項目(2/4)

醫學中心 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112 年度醫院評鑑基準及評量項目(醫學中心適用)		
條號	條文	評量項目
1.4.9	具備資訊管理作業規範，以確保資訊安全及維護病人隱私，並訂有緊急應變處理機制	**符合項目：** **1. 依「資通安全管理法」，資通系統應有資訊系統使用權限設定及防止資料外洩之資訊管理相關作業規範，並具備資訊安全管理機制(如：資訊需求申請程序書、資訊系統密碼管理辦法、程式撰寫文件管理辦法、資訊系統備份作業程序書、資訊安全稽核作業程序書、網路頻寬使用管理辦法、網際網路使用規範、網路信箱管理辦法等)。(原 1.5.9-符合 1 修)** **5.訂有資訊系統故障(當機)、資通安全事件及個資事件緊急應變標準作業規範。(原1.5.9-符合5修)**

112 醫院評鑑說明會

醫學中心醫院評鑑基準及評量項目(3/4)

醫學中心 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112 年度醫院評鑑基準及評量項目(醫學中心適用)		
條號	條文	評量項目
1.4.9	具備資訊管理作業規範，以確保資訊安全及維護病人隱私，並訂有緊急應變處理機制	**符合項目：** 6.訂有資通安全維護計畫並有加入衛生福利部資安資訊分享與分析中心(H-ISAC)會員，並適時進行情資分享，提升其資通安全維護能量，調整資通安全應變機制，預防相關資通安全威脅之發生。(試)

醫院評鑑說明會

醫學中心醫院評鑑基準及評量項目(4/4)

醫學中心 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112 年度醫院評鑑基準及評量項目(醫學中心適用)		
條號	條文	評量項目
1.4.9	具備資訊管理作業規範，以確保資訊安全及維護病人隱私，並訂有緊急應變處理機制	**優良項目：** **1.針對核心資通系統故障緊急應變計畫進行演練，並有故障原因和處理紀錄檢討改善。(原1.5.9-優良1修)** 4.核心資通系統導入資訊安全管理系統標準(如：ISO27001、CNS27001或其他具有同等或以上效果之管理系統或標準)及公正第三方檢驗，並持續維持其驗證有效性。(試) **評量方法及建議佐證資料：** 4.醫院資訊系統故障(當機)、資通安全事件及個資事件緊急應變標準作業規範與程序。(符合) 5.資通安全維護計畫及實施情形文件紀錄。(符合) 6.電腦系統故障演練紀錄與資訊安全事故報告單、資通安全事件通報單與處理紀錄(或演練通報檢討紀錄)。(優良) 9.通過 ISO27001、CNS27001 或其他具有同等或以上效果之管理系統或標準之證明文件。(優良)

醫院評鑑說明會

區域醫院、地區醫院 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112年度醫院評鑑基準及評量項目(區域醫院、地區醫院適用)		
條號	條文	評量項目
1.4.3	資訊部門配合臨床及行政部門建立完善作業系統，且院內各系統連線作業及院外聯繫系統功能良好	**符合項目：** 3..設有資訊安全管理委員會或相關組織，負責資訊安全工作推動及追蹤，訂有資訊安全管理計畫且召開跨部門之管理會議，能針對資安列管設備(含醫療儀器及其他支援設施)、臨床與行政決策系統進行討論，落實資訊安全以確保病人安全及提升醫療品質。 **[註]** 2.若通過「醫院緊急醫療能力分級評定」並於重度級急救責任醫院合格效期內者，應設立資通安全長，並由現任副院長以上層級人員擔任。 **3.符合項目2、3申請「地區醫院評鑑」者可免評。** **評量方法及建議佐證資料：** 5.資訊安全管理委員會或相關組織之章程與會議紀錄。(免) 6.資訊安全管理年度計畫。(免)

醫院評鑑說明會

區域醫院、地區醫院 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112年度醫院評鑑基準及評量項目(區域醫院、地區醫院適用)		
條號	條文	評量項目
1.4.4	具備資訊管理作業規範，以確保資訊安全及維護病人隱私，並訂有緊急應變處理機制	**符合項目：** 1.依「資通安全管理法」，資通系統應有資訊系統使用權限設定及防止資料外洩之資訊管理相關作業規範，並具備資訊安全管理機制(如：使用者權限界定、資訊需求申請程序書、資訊系統密碼管理辦法、程式撰寫文件管理辦法、資訊系統備份作業程序書、資訊安全稽核作業程序書、網路頻寬使用管理辦法、網際網路使用規範、網路信箱管理辦法等)，以確實保障病人個人隱私。 4.訂有資訊系統故障(當機)、資通安全事件及個資事件緊急應變標準作業規範。針對資訊系統故障緊急應變計畫進行演練，並有故障原因和處理紀錄檢討改善。

醫院評鑑說明會

區域醫院、地區醫院 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112年度醫院評鑑基準及評量項目(區域醫院、地區醫院適用)		
條號	條文	評量項目
1.4.4	具備資訊管理作業規範，以確保資訊安全及維護病人隱私，並訂有緊急應變處理機制	**符合項目：** **5.訂有資訊系統風險管理計畫，且主動積極進行風險分析、監測及管理，並落實執行，可被廣泛應用。** 6. 訂有資通安全維護計畫，且有加入衛生福利部資安資訊分享與分析中心(H-ISAC)會員，並適時進行情資分享，提升其資通安全維護能量，調整資通安全應變機制，預防相關資通安全威脅之發生。(試) **[註]** 4.符合項目6列為試評項目，評量結果不納入評鑑成績計算。 5.符合項目5申請「地區醫院評鑑」者可免評。

醫院評鑑說明會

區域醫院、地區醫院 112 年度醫院評鑑基準及評量項目-修正

第1篇、經營管理 第1.4章 病歷、資訊與溝通管理

112年度醫院評鑑基準及評量項目(區域醫院、地區醫院適用)		
條號	條文	評量項目
1.4.4	具備資訊管理作業規範，以確保資訊安全及維護病人隱私，並訂有緊急應變處理機制	**評量方法及建議佐證資料：** **5.醫院資訊系統故障(當機)、資通安全事件及個資事件緊急應變標準作業規範與程序。** **6.電腦系統故障演練紀錄與資訊安全事故報告單、資通安全事件通報單(或演練通報檢討紀錄)。** **8. 資通安全維護計畫及實施情形文件紀錄。**

醫院評鑑說明會

感謝聆聽

Thank you for your attention