調　查　報　告

壹、案　　由：據悉，國內部分醫療院所多次發生資安事件，基於醫療體系為我國八大關鍵基礎設施領域之一，經管個資更屬「個人資料保護法」所定之特種個資，資安風險影響醫療品質、病人安全、民眾隱私及國安甚鉅，究主管機關及醫療機構如何協助及確保風險識別、資安法遵、通報應變及情資分享？資安主管機關提供之輔導協助是否適足？醫院評鑑有無涵蓋資通安全事項情形等，均有深入瞭解之必要案。

貳、調查意見：

本案經調閱衛生福利部（下稱衛福部）卷證資料，並於民國(下同)112年12月21日及28日分別現場履勘部立桃園醫院、彰化基督教醫院及中國醫藥大學附設醫院，並於113年3月26日詢問衛福部及所其所屬機關人員，已調查完畢，茲臚列調查意見如下：

一、根據「資通安全責任等級分級辦法」及「資通安全事件通報及應變辦法」規定，醫療院所事前應對資通系統進行防護需求分級，事中應變則依規定進行通報；惟查各醫療院所之資通系統防護需求分級、納列情形及資安事件通報觸發條件及等級認定等均有相當歧異，究其原因，不無醫學中心或關鍵基礎設施提供醫院分屬不同主管機關等因，實有肇生風控落差及不利大規模事件聯防之虞，爰應檢討改進，主管機關衛福部允宜善用資安長交流機制及醫療評鑑等工具予以強化，並針對人力資源問題提供協助。

(一)在「資通安全管理法」各子法所建構之事前預防、事中應變及事後復原之法遵架構中，「資通安全責

任等級分級辦法」主要屬於事前預防層面，而「資通安全事件通報及應變辦法」則屬於事中應變層面。

1、「資通安全責任等級分級辦法」第2條規定:「公務機關及特定非公務機關之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。」;復依第11條第2項規定:「各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施」;換言之，無論醫療院所為公務機關或特定非公務機關，或屬於哪一個主管機關，其資通系統均應完成資通系統防護需求等級之分級。

2、其次，「資通安全事件通報及應變辦法」第2條，則將資安事件分為四級，各分級的構成要件訂於第2條第2至5項，以醫療院所較常見之「二級事件」及「三級事件」為例，其構成要件如下；換言之，各醫療院所必須事先認定資通系統是否屬於「核心業務」，嗣於通報時研判其事件嚴重程度。

（1）二級事件：各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件。

〈1〉非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

〈2〉非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

〈3〉非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統

之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

（2）三級事件：各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件。

〈1〉未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

〈2〉未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

〈3〉未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

(二)經查，受衛福部納管的公務機關為部屬醫院，該部為其上級機關；至於納管之非公務機關，係由衛福部擇定特定非公務機關關鍵基礎設施提供者(CI醫院)，並經行政院核准。另臺灣大學附設醫院及成功大學附設醫院以教育部為上級機關，臺北、臺中及高雄榮民總醫院以退除役官兵輔導委員會為上級機關；經查其資通系統防護需求等級納列情形，可以發現存在「納列防護需求的資通系統數量十分懸殊」、「部分院所之核心業務資通系統似未將防護需求等級列為『高』」、「多數院所對於防護等級『中』以下之資通系統未經第三方驗證」等三項疑義，值得衛福部進一步檢視其法遵及合理性。

1、該部所管關鍵基礎設施提供者(13家私立醫學中心)、26家所屬醫院，以及教育部所管2家醫學中心、國軍退除役官兵輔導委員會所屬3家醫學中心之資通安全責任等級分級情形如下：

（1）「資通安全責任等級分級辦法」第4條第7款規定，公立醫學中心資通安全責任等級為A級；同辦法第5條第7款規定，公立區域醫院或地區醫院資通安全責任等級為B級。

（2）醫學中心（私立醫院）之責任等級，比照公立醫院，為A級。

（3）衛福部附屬醫療院所屬公立區域醫院或地區醫院，資安責任等級為B級。

2、其次，醫療院所之資通系統分級情形如下，一般而言，若有資通系統漏未列入分級或等級不適當情形，則該資通系統將因風險未受適當控制而暴險：換言之，資通系統之資安分級情形代表著院所對於自身資安風險之事前預防工作及認知是否完善；茲以衛福部所管私立醫院、部立醫院、教育部及輔導會所管醫院共44家醫院為例，臚列其資通系統防護需求分級情形如下表27:

表1　衛福部、教育部及輔導會所管醫療院所資安責任等級及核心業務資通系統防護需求等級。

主管部會	醫療院所	資安責任等級	資通系統防護需求分級數量			
			高	中	普	合計
衛福部	○○醫院	A	3	4	42	49
	○○醫院	A	3	0	5	8
	○○醫院	A	5	0	1	6
	○○醫院	A	3	0	5	8
	○○醫院	A	5	0	11	16
	○○醫院	A	8	0	21	29

	○○醫院	A	3	0	10	13
	○○醫院	A	4	0	8	12
	○○醫院	A	2	4	2	8
	○○醫院	A	6	8	1	15
	○○醫院	A	3	14	12	29
	○○醫院	A	3	12	9	24
	○○醫院	A	1	1	1	3
部屬醫院	○○醫院	B	3	4	3	10
	○○醫院	B	3	2	0	5
	○○醫院	B	3	4	10	17
	○○醫院	B	3	2	5	10
	○○醫院	B	3	0	0	3
	○○醫院	B	1	0	3	4
	○○醫院	B	1	4	2	7
	○○醫院	B	2	1	0	3
	○○醫院	B	3	4	0	7
	○○醫院	B	5	4	1	10
	○○醫院	B	3	4	5	12
	○○醫院	B	4	0	0	4
	○○醫院	B	2	1	5	8
	○○醫院	B	2	3	1	6
	○○醫院	B	1	2	2	5
	○○醫院	B	2	2	7	11
	○○醫院	B	5	10	14	29
	○○醫院	B	2	4	5	11
	○○醫院	B	1	0	7	8
	○○醫院	B	2	11	1	14
	○○醫院	B	2	2	5	9
	○○醫院	B	2	2	0	4
	○○醫院	B	2	10	8	20
	○○醫院	B	3	0	0	3
	○○醫院	B	3	4	3	10
	○○醫院	B	4	0	15	19
教育部	○○醫院	A	10	2	1	13
	○○醫院	A	2	5	42	49
輔導	○○醫院	A	3	3	1	7

會	○○醫院	A	3	2	2	7
	○○醫院	A	2	0	4	6

3、以上表醫療院所為例，其防護需求分級之納列有以下情形值得注意:

（1）納列防護需求的資通系統數量十分懸殊：在資安責任等級同為A級之醫療院所中，有2家院所(新光醫院、臺中榮總)僅納入6個資通系統，亦有2家院所(國泰醫院、成大醫院)納入高達49個資通系統；如以一般統計學上用以描述數據離散情形之指標如標準差(SD)及變異係數(CV)而言，更分別高達13.9及184.8;縱考量各醫療院所之規模、資通系統架構、系統整併情形及所選用之服務有相當差異，各院所納列防護需求等級情形仍十分懸殊，其中恐有納列未臻合理之情況,值得衛福部整體評估或提供院所指引。

（2）部分院所之核心業務資通系統似未將防護需求等級列為「高」:按照衛福部於109年於臺灣資安大會(CYBERSEC2020)簡報，已規劃將醫療核心資通系統導入ISO27001，其中所謂「核心資通系統」係包括諸如檢驗系統(LIS)、電子病歷系統(EMR)、醫療影像系統(PACS)、處方系統(PIS)、護理系統(NIS)等等；然而就衛福部提供之資料顯示，雖然多數院所均將前述核心資通系統防護等級列為「高」且依資安法通過第三方驗證，然仍有部分院所未將核心資通系統防護等級列為「高」,例如國泰醫院之PACS及LIS系統、萬芳醫院NIS系統以及高醫大LIS系統等;另外部屬醫院同質性相對較高，然而亦可發現部分院所之護理系統(NIS)列為「高」，而部分院所則列為「中」;其中雖然可能因其系統設計

或服務而毋須列為核心業務資通系統；然而鑒於本院過去調查部分政府機關資安事件，如銓敘部案(109教調0004)及公視數位片庫案(111教調0040)之根因，即為低估資通系統防護需求等級，是以相關院所核心業務資通系統之防護需求基準是否妥適，值得衛福部進一步探究，對此，衛福部吳美琪科長於本院113年3月26日辦理詢問時回應如下，顯示衛福部亦認有改進空間。

〈1〉例如EMR和HIS、PACS，核心系統有兩個定義，一是支持核心業務運作的系統，另是依照「機密性」、「完整性」、「可用性」及「法遵性」等四個面向而予以分級；如有沒納入的，我們會要求改善。

〈2〉【問:看起來有些院所的PACS只列為普?】我們會逐步跟醫院溝通，希望該列高的要列為高。

（3）多數院所對於防護等級「中」以下之資通系統未經第三方驗證：經查，所有院所對於防護等級「高」之資通系統均有通過第三方驗證，然而大部分院所在防護等級「中」以下之資通系統均未經第三方驗證，似為後續可精進之方向之一。

(三)在資通安全事件通報等級方面，由於「資通安全事件通報及應變辦法」相關規定具有不確定法律概念，故無法直接依照字面辦理；而根據本院112年12月28日辦理履勘發現，不同院所對於資安事件通報之觸發條件及等級認定，已各自發展出不同規則如下，部分院所規則較為嚴謹，而部分院所規則略顯簡要，將可能造成同一類型或等級之事件，各院所

通報情形不一之情形，對於大規模事件之聯防恐有不利，衛福部允宜透過資安長交流機制，對各院所建立之規則進行交流參考，以促使各醫療院所截長補短，將通報實務趨向最佳實踐(best practice)。

1、根據本院112年12月28日履勘彰基醫院及中國附醫之通報觸發條件及等級認定規則如下:

（1）以彰基醫院為例，該院對資安事件之定義(觸發條件)為「受影響設備數30%以上且停頓30分鐘以上」

（2）若以中國附醫為例，該院對資安事件訂有配分表如下表，其計算方式為「資訊異常事件等級=A+B+C，比0小則視為 0，比4大視為4」，觸發通報機制之條件則為「若等級為0屬於資訊異常事件，由醫院自行處理;若≧1，則通報H-ISAC」。

表2　中國附醫資安事件通報及等級認定配分表。

<table>
<tr><td>分類</td><td>配分</td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="6">A</td><td>4</td><td>國家機密</td><td colspan="2" rowspan="3">資料類</td></tr>
<tr><td rowspan="2">3</td><td>一般公務機密</td></tr>
<tr><td>敏感資訊</td></tr>
<tr><td rowspan="3">0</td><td>業務資訊</td></tr>
<tr><td>資通系統</td><td colspan="2">系統類</td></tr>
<tr><td>業務運作</td><td colspan="2" rowspan="2">運作類</td></tr>
<tr><td>資通系統運作</td></tr>
<tr><td rowspan="4">B</td><td>3</td><td colspan="3">涉及關鍵基礎設施維運之核心</td></tr>
<tr><td>2</td><td colspan="3">未涉及關鍵基礎設施維運之核心</td></tr>
<tr><td>1</td><td colspan="3">非核心</td></tr>
<tr><td>0</td><td colspan="3">if A ≠ 0</td></tr>
<tr><td rowspan="2">C</td><td></td><td>資料類</td><td>系統類</td><td>運作類</td></tr>
<tr><td>1</td><td>遭嚴重洩漏/竄改</td><td>遭嚴重竄改</td><td>無法於可容忍中斷時間內回復</td></tr>
</table>

	0	遭輕微洩漏/竄改	遭輕微竄改	於可容忍中斷時間內回復
	-4	沒有遭洩漏/竄改	沒有遭竄改	沒有受影響或停頓

2、對此，衛福部李建璋處長於本院113年3月26日辦理詢問時表示：「（通報）主要是本部在把關，之後我們會找專家委員會來訂一個原則，之後也會設計在通報系統表單中，使醫院有所遵循」，顯示衛福部已有相關精進規劃，此外，李建璋處長對於隱匿通報之可能性則表示，該部除既有法定之通報機制以外，亦有暗網情資及政府聯防體系之通報為輔，尚不致有發生災情時無法掌握之情形。

3、此外，中國附醫之通報機制考慮相對周詳，包括將對外溝通及技術處理人員分開配置、線上會議紀錄及保留紙本SOP等等，均有值得其他院所參考之處，主管機關允宜透過適當交流機制分享。

4、對於前揭「資通安全責任等級分級辦法」及「資通安全事件通報及應變辦法」各院所實務操作之差距，衛福部周志浩次長於本院3月26日辦理詢問時總結：「這是長期以來的挑戰，因為它預算、人事都是其他部會管理，如果體系無法調整，我們就是依據相關法令來規管，我們要發揮法令中賦予的權力，此外也要依賴跨部會的協調。衛福部主要是靠這兩個工具」等等；周志浩次長進一步說明，如要進行跨部會協調，則「跨系統有CI醫院，都是以CI為架構，每年都有資安長會議，另外聯防體系也有跨部會的通報，另外在攻防演練和稽核方面，我們也會進行跨部會，簡言之，醫療體系資安是靠CI為中心來組建的」，顯示衛福部應積極利用既有機制，對於各院所差異懸殊

或有待分享之作法進行妥處。

(四)另查，依據本院履勘時醫療院所反映，多數院所均遭遇資安人力問題及通報應變機制之挑戰，茲將相關建議及問題臚列如下，主管機關允宜加以正視，俾強化院所之資安風控能力。

1、在資安人力問題方面，部分院所反映「若『資通安全責任等級A級之特定非公務機關應辦事項』之資通安全專責人員改成資通安全專職人員，私立醫療院所聘請合規人員壓力極大」，其他院所則無論是資訊部、醫工部或工務部均反映現有人力不足之窘境。

2、此外，院所亦反映，目前通報應變辦法尚未針對「被入侵、未發作、自主發現」之樣態制定通報規定，基於資安聯防之考量，主管機關允宜針對該等樣態建立適當之通報規則。

3、對此，衛福部李建璋處長於本院113年3月26日辦理詢問時表示，「醫院成本已經被四面八方的壓縮，但即使如此，例如現在採購案一定要有5~10%比例經費是資安項目，未來評鑑也會研議納入重要項目，資安相關規範會對接紐約州的精神。中小型醫院沒有人力，我們預計依賴聯防機制，讓大醫院帶小醫院」，則該部後續宜有明確精進作法。

(五)綜上，自108年資通安全管理法施行以來，我國資安法遵事宜日趨嚴謹而繁複，而其事前風險認知周妥與否，則能相當程度反映醫療院所對於資安風險之認知程度及準備情形；經查國內醫療院所在事前之資通系統防護需求等級納列及事中應變之通報條件及機制，即便考量各院所規模、資通系統架構、服務及系統整併等等因素，其實務作法之差異仍十

分懸殊，將容易造成各院所之風控落差及聯防體系漏洞等問題，爰有檢討必要，而衛福部既對相關問題亦有所認知，則允宜研謀具體措施予以強化，並針對院所遭遇之挑戰提供充分協助及指引。

二、醫療儀器將因未來智慧及數位醫療趨勢而愈形重要，惟多數醫療儀器具備工業控制系統(Industrial Control System ，ICS)及營運技術(Operation Technology，OT)特性，其資安管理尚未如資訊技術(Information Technology，IT)成熟，較易遭遇漏洞更新或供應鏈廠商之資安風險，衛福部縱已較其他關鍵設施領域積極制訂相關指引，惟查各醫療院所對指引之解讀及醫療儀器之資安資產認定仍有相當歧異，爰有檢討必要，復以各醫療院所之第三方或第二方稽核難以精確評估醫儀之工控風險，衛福部允宜提供額外協助，以適當控管未來智慧及數位醫療將遭遇之資安風險。

(一)根據2023年行政院生技產業策略諮議委員會議簡報顯示，數位醫療產業營業額每年成長10%以上，2022年已達新臺幣502億元之規模，衛福部並於會中宣示加速醫療資訊系統革新，置重點於「系統的互通性」、「行動整合解決方案」、「資訊數位化」、「安全的通信系統」、「穩定的核心基礎設施」、「系統自動化」等六點；至2024年3月美國新聞週刊(Newsweek)所排名之全球最佳智慧醫院中，國內已有四家醫院(臺中榮總、中國附醫、臺大醫院及臺北榮總)獲得佳績[1]，足見智慧及數位醫療已為未來趨勢。而隨之衍生之資安風險，於資產面一般分為IT及OT資產，

[1] 天下雜誌。2023年9月23日。2024全球最佳智慧醫院　中榮二度入榜，中國醫、台大、北榮首度入列。https://futurecity.cw.com.tw/article/3189

茲就OT部分之資安重要性臚陳如下：

1、根據衛福部109年8月17日訂頒之「基層醫療院所資安防護參考指引」中指出，醫院該注重的資安範圍不只是IT(Information Technology)，還包括OT（Operation Technology，操作型技術）的安全，也就是醫療儀器。近年來各家醫院紛紛發展智慧醫療4.0，利用大數據、AI、雲端和IoT技術分析醫療資料、開發新服務，甚至發展遠距照護和個人化基因分析。

2、為了推動智慧醫療、加速醫療資料的傳輸與分析，醫院勢必採用可連線的醫療儀器，但這也成為資安隱憂。醫療資安防護不只要把個人電腦和伺服器管理好，還要注重醫療儀器的資安檢測，比如護理工作車、電腦斷層掃描設備、醫療檢測儀器等。

(二)在行政院國土安全政策會報107年11月發布之「關鍵資訊基礎設施資安防護建議」中，針對工業控制系統(ICS)提出通用性防護建議，其中更敘明，工業控制系統高度強調可用性，而一般資通系統較重視機密性，兩者在功能設計理念具有相當大的差異，因此工業控制系統(ICS)無法完全套用已建立的資訊技術(IT)資安防護相關標準或建議。且工業控制系統廣泛使用於能源、交通、**醫療**及製造等領域，**各領域的工業控制系統會因領域不同而有其特殊性**，其資安防護須依領域進行調整，顯見ICS及OT之資安議題，必須與IT分別看待。

(三)基於醫療儀器資訊化及數位化甚為普遍及多樣，衛福部對於營運技術(OT)之資安風險意識及控制措施，與各部會相較尚屬進步(另經濟部亦早於108年12月10日即發布「工控物聯網共通性資安指

南」），其政策大致可分為醫療儀器上市前針對業者進行規範，以及醫療院所使用後之院內風險管理。

1、該部108年公告「適用於製造廠之醫療器材網路安全指引」，110年修訂公告「適用於製造業者之醫療器材網路安全指引」，該指引調和國際標準、國際組織、先進國家指引等要求以確保聯網醫療器材之網路安全。又公告指引前該部對於可資料傳輸之醫療器材於查驗登記時，除業者需檢附相關軟體確效文件外，其醫療器材製造業者在醫療器材品質管理系統下應執行產品生命週期之風險評估，建立風險管理流程識別包含網路安全之相關危害並確保風險管控措施的有效性。

2、其次該部參照資通安全責任等級分級辦法附表十資通系統防護基準，訂定「醫療領域資通系統資安防護基準」，並於112年11月8日函知各醫療機構。醫療領域防護基準共有10個控制構面、36個控制目標及75個控制措施，分別針對網路架構、存取控管、事件日誌、營運持續計畫、系統與通訊防護、實體與環境防護等面向進行控管，藉由IT及OT人員配合確認列管設備、聯網方式與架構，評估防護需求等級並套用對應之防護控制措施。

（1）10個控制構面包括：網路架構、存取控制、事件日誌與可歸責性、營運持續計畫、識別與鑑別、系統與通訊防護、系統與服務獲得、實體與環境防護、系統與資訊完整性、組態管理及組織管理。

（2）在醫療儀器資安分群分類模型部分，將儀器分為終端儀器群及控制系統群；其中終端儀器群

再分為終端單機(如護理推車)、群組型儀器(如生理監視器)及系統型儀器(如CT或MRI)；控制系統群指規格上可連線管理2台（含）以上「終端儀器」群之單機或邊界主機，連結院內系統網路（Intranet） 傳輸資料之臨床儀器控制系統，包含「醫儀控制系統」與「醫儀應用系統」二類。

〈1〉醫儀控制系統：全稱為「醫療儀器資訊控制系統」，指控制「終端儀器」的管理系統；只管理「儀器ID」及「檢驗檢查資料」；不落地儲存與醫療機關資訊系統交換的「可識別資料」、不管理資料查詢的「醫事人員帳密權控」;功能上不涉及識別個人資訊的控制軟體系統。如：ICU生理監護系統伺服器主機、洗腎機拋轉系統設備伺服器的控制軟體系統。

〈2〉醫儀應用系統：全稱為「醫療儀器資訊應用系統」，指「終端儀器」的控制應用管理系統；包含交換且儲存HIS病人個資資訊、有管理醫事人員帳密權控等可識別資訊的儀器控制及連結臨床應用套裝軟體系統。如：產房資訊系統、檢驗備管系統伺服器的應用軟體系統。

（3）現已針對醫療領域防護基準擬定查檢表，將請醫院自評確認目前達成情形，並於實地稽核時檢視落實情形。

(四)按資通安全管理之程序一般可分為識別、保護、偵測、回應及復原，換言之，防禦必須從了解「有哪些資產」以及「守備邊界為何」等風險識別開始；惟查，根據衛福部於113年3月26日本院辦理約詢前所提供之醫療院所OT資產盤點情形，發現各院所實

際盤點情形極為懸殊，包括地區醫院共盤點出372項OT資產，而醫學中心只盤點出5項OT資產；此外也發現有醫療院所將「核子醫儀」與「身高體重計」之風險等級都同樣列為普級，顯示各醫療院所對於「醫療領域資通系統資安防護基準」之解讀及OT資產之認定標準差異甚鉅，亟待衛福部協調妥處，茲將研析發現臚列如下。

1、在醫儀認定為是否為OT資產之標準方面，以教育部所管臺大醫院為例，該院為關鍵基礎設施且為資通安全責任等級A級機構，其醫儀共納列5項OT資產，包括「無線連線型生理監視器」(364台)、「重症用生理監視器」(283台)、「心電圖機」(109台)、「MRI」(6台)及「CT」(7台)等5項，而衛福部所屬彰化醫院為資通安全責任等級B級機構，卻納列了372項醫儀為OT資產，包括一般常被列為OT資產的生理監視器，但也包括血壓計、電子身高體重計及抽痰機等設備；顯見即使衛福部已訂頒「醫療儀器資通系統資安防護基準」共10個構面作為醫療院所認定OT資產之依據，但在不同主管機關所屬之醫療院所內，對於哪些設備應視為OT資產，仍有極為巨大的認知差距。若醫療院所之OT資產認定過於嚴謹，將可能因漏列資產而任由醫儀更新漏洞持續存在而形成駭客入侵管道；反之，認定過於寬泛則造成未來管理、更新及通報之行政成本過高，亦非最佳實踐（best practice)，爰有檢討必要。

2、在認定為OT資產後，院所尚需進一步依照衛福部所訂頒之防護基準對OT資產之資安風險進行分級；惟查部分院所在風險分級的合理性方面尚有疑義，以教育部所屬成大醫院為例，「坐式磅秤」

與「正子暨電腦斷層造影機」之資安風險同樣為普級；而在衛福部所屬臺東醫院，「糖化血色素分析儀」亦與「磁振照影儀(MRI)」同樣被列為普級；值得衛福部進一步針對各院所在系統防護需求分級方面之合理性進行分析，避免因嚴謹程度不一而有形成木桶理論[2]之虞。

3、此外，本院亦發現有相同OT資產(醫儀)在不同院所所認定之資安風險不同之現象；以教育部所管成大醫院為例，該院「內視鏡主機(含光源機及影像系統)」風險列為普，然輔導會所屬臺中榮總，其「內視鏡影像系統(主機)」卻列為中，則其資安風險在「醫療儀器資通系統資安防護基準」10個構面(網路架構、存取控制、事件日誌與可歸責性、營運持續計畫、識別與鑑別、系統與通訊防護、系統與服務獲得、實體與環境防護、系統與資訊完整性、組態管理及組織管理)評估後是否確有風險等級差異，有待進一步檢視。

(五)承上，在過去本院調查銓敘部(109教調0004)及基隆市教網中心(113教調0007)等案時，均曾指出資通安全委外輔導驗證廠商之問題；基於衛福部資料顯示各醫療院所之資訊安全輔導驗證均委外辦理，復以「OT設備之資安輔導驗證尚不如IT成熟」、「醫儀形式種類極為繁複」以及「輔導驗證廠商利益衝突或素質參資不一」等因，將來勢難避免OT設備通過輔導驗證，但事實上仍未適當風控而不斷發生資安事件之情形，值得衛福部先行研謀對策。

(六)對此，衛福部李建璋處長於本院113年3月26日辦理約詢時表示：「**OT部分確實特別繁複，連資安專家都**

[2] 指整體能力之高低，取決於構成要素中最弱的一環。

很難擬定作法」、「我們會有清單系統盤點，但一直會有新形態的設備進來，稽核也未必有這麼仔細，所以都還是要靠稽核和防火牆來發現等語」，李處長並補充，「現在在智慧醫療都會取得重要資訊來做人工智慧，行政院目前只規範公立醫院禁用陸廠資通產品，我們只能規範聯網設備必須要有防火牆和防毒，未來會同步納入私立醫院去檢視陸廠設備有無資安問題。」等語，顯見OT問題確為衛福部、相關機關及醫療院所未來必將面對的挑戰。

(七)綜上，醫療院所醫儀設備多具OT及ICS系統特性，但OT系統之資安管理未如IT系統成熟，衛福部縱已積極控管資安風險並訂定指引，惟調查發現各醫療院所對於「醫療領域資通系統資安防護基準」之解讀差異甚鉅，已有構成資安風險之虞，復以委外輔導驗證之資安廠商亦難以充分控制其風險，綜合上述情況，將造成院所本身(第一方)及輔導驗證廠商(第三方)均難以充分控制風險，而在智慧及數位醫療快速普及的趨勢下，其風險將進一步加劇，尚賴衛福部善用法令及政策工具，如關鍵基礎設施或醫院評鑑等，以協調各主管機關(第二方)積極改善。

三、部立桃園醫院自109年起陸續發生資安事件，其中於111年護理系統傳出遭駭事件，經鑑識後雖釐清為磁碟陣列故障導致，但也意外查出系統遭植入挖礦軟體之案外案；該院一連串之資安事件雖已進行懲處及檢討改進，惟衛福部允宜持續督導促其改善；此外，基於資安管理重點已由事前防堵逐漸轉向事中應變及事後復原，以近期CrowdStrike及英國Synnovis事件為例，更凸顯在雲端服務快速普及之下，供應鏈安全、事中應變及事後復原將日益受到重視，亦值衛福部及資通安全主管機關重視並預先擬定對策。

(一)根據衛福部112年8月28日衛部資字第1122660426號函提供資料說明，部立桃園醫院自109年以來數起資安事件之始末如下：

1、109年8月發生駭客利用WebShell漏洞感染12台主機事件:經桃園醫院資安服務廠商安碁資訊股份有限公司（下稱安碁公司）鑑識，發生原因為院內多部端點遭反覆感染惡意程式，而該惡意程式係屬「蠕蟲」。該院電腦全數採用趨勢防毒軟體，相關契約為衛福部所屬醫院聯合採購契約訂定，當時趨勢防毒軟體並未偵測到該病毒，以致無法即時防範致院內多部端點遭感染。

2、110年2月桃園醫院由奧義智慧端點防護監控到4部端點存在惡意程式，經安碁公司鑑識，本案肇因為含病毒隨身碟在3台電腦間插拔。事件後，該院採行全面禁止使用可攜式儲存裝置。至111年9月起，為平衡資安管控及行政需求，始調整為行政單位及會議室，如有業務使用上之必要性，可經申請後開通使用。112年3月導入主動式資安防護，針對可攜式儲存裝置安裝加密軟體（USBVES)，防止機密資料外洩。

3、110年5月網路防火牆設定錯誤，導致遭外部暴力破解嘗試植入惡意程式。

（1）本次事件始於奧義智慧戰情中心通報桃園醫院兩部主機遭受攻擊，該院隨即通知安碁公司派員鑑識。

（2）事件根因分析包括:防火牆規則未落實管控，以及本機防火牆未針對特定服務限定來源存取等，屬於人員設定疏漏之內控問題。

4、111年3月桃園醫院發現護理系統(NIS)無法使用，NIS資料庫疑似遭到刪除等，該院隨即通知數

聯資安公司進行鑑識，並通報前行政院資安會報技術服務中心(簡稱技服中心，現改制為資通安全研究院)支援。

（1）經鑑識，數聯資安公司及前技服中心均認NIS資料庫無法存取係因磁碟陣列故障導致，並非遭到駭侵刪除。

（2）然而數聯資安公司及前技服中心均查出NIS資料庫主機早於110年5月即遭駭侵植入挖礦程式。

（3）據鑑識，110年時，端點偵測軟體並不支援LINUX系統，以致該主機並未於SOC防護範圍。鑑於該缺失，該院於衛福部新一期聯合採購內，即提出新的SOC案端點防護軟體需支援LINUX系統。

（4）本案另發現桃園醫院自109年起，未與廠商簽訂NIS維護合約，衛福部說明，桃園醫院資訊室進行單位驗收時，為求審慎提出需繳交最高權限帳號等數項資料，故與廠商間針對驗收項目有所歧見，致該維護契約未驗收完畢。考量系統維運順暢，該院持續徵求維護廠商，此期間公開招標2次護理資訊系統維護案，均無廠商投標。

(二)衛福部補充有關前開資安事件之責任檢討情形如下：

1、桃園醫院自111年1月起陸續發生數起資安事件，且未依資安法規定通報、應處逾時，經衛福部多次去函要求限期改善，並提報檢討報告，惟該院多次逾期回復，爰衛福部於111年6月22日去函，請該院提報檢討報告及懲處名單陳報。

2、衛福部桃園醫院於111年7月25日15時召開第5次

甄審及考績委員會，並請案內相關人員列席報告，該次會議未作出懲處之決議。111年8月4日召開111年度第7次甄審及考績委員會，會前請政風室協助調查資訊室辦理資安事件逾期通報及公文屢次未依限函復上級機關，涉有行政疏失一事。經審酌資安長及資安專責人員陳述意見、事實證據以及政風室調查結果，委員會作成決議如下：

（1）資安人員連○芬組長部分：連員承辦資安事件相關函文計有6件，其中5件已逾上級機關所定回復期限，因其行政效率不彰，多次延宕公文辦理時效之情形，決議核予申誡1次處分並調離現職。

（2）資安人員呂○超組長部分：呂員承辦資安事件相關函文計有2件，皆已逾上級機關所定回復期限，就其行政效率不彰，延宕公文辦理時效之情形，決議核予申誡1次處分。

（3）資訊室主任呂○巍資訊師：呂員111年4月21日起至同年7月18日止擔任資訊室主任期間，多份公文延宕，呂員未督促所屬同仁並積極跟催逾期公文辦理情形，致該院聲譽受損，因呂員認知資安相關業務非屬其職務範疇，部分案件公文流程確未經其核章，爰決議核予書面警告處分，以資警惕。

（4）資安長陳○全醫師兼副院長：陳員對業務嚴重督導不力部分，免兼其資安長職務，並依衛生福利部所屬醫療機構醫事人員兼任院長副院長及各級醫事主管之任期及遴用辦法第18條第1項之規定，將案件相關內容作為年度評核之參考，陳報衛福部辦理。

3、經衛福部111年8月31日去函，就資安長懲處部分，咸認為理由陳述不夠具體明確，請該院重新檢討。爰該院重新展開調查，並蒐集相關事證，於111年9月15日召開111年度第9次甄審及考績委員會，並請該員列席陳述意見，因案情複雜，當次會議因時間限制未審議完成，於隔（16）日召開第10次甄審及考績委員會，經與會委員審慎討論，認為陳員有未依上級指示辦理資安業務、未參酌所屬或第三方專業意見，對資安業務為適切之判斷及指示、未積極督導所屬資訊部門辦理資安業務等違失，對於整體資安業務有督導不力之情事，決議核予陳員記過一次處分。

4、陳員因不服上開處分結果，於111年10月7日提起復審，請求撤銷原處分，並主張該院未給予其陳述意見之機會，其無督導不周之情事，案經公務人員保障暨培訓委員會於112年3月21日112公審決字第000088號復審決定書，認陳員在所掌督導資訊業務工作方面，核有造成不良後果，情節較重大之情事，該院依相關規定核予記過一次處分，並無違誤，爰作成復審駁回之決定。

(三)衛福部認為桃園醫院資安事件較其他部立醫院頻繁之原因探討包括:

1、桃園醫院相較於其他部立醫院，除具準醫學中心規模，業務量龐大。

2、該院資安事件統計，111年通報11件，除來自國家資通安全研究院入侵事件警訊通報3件外；另自行發現的異常事件8件也都納入通報，爰通報件數相較其他醫院為多。經分析為承辦人員不諳程序致有逾時通報3件，後續該員已受懲處，並調離現職。再查112年迄今通報4件，除來自國家資通

安全研究院入侵事件警訊通報1件外；另自行發現的異常事件通報3件已無逾時現象。可見**不適任人員調離後，通報缺失已明顯改善**。

(四)另查，過去資安管理較偏重事前防堵，而事中應變及事後復原則較不受重視，此為網路防禦矩陣(CDM，Cyber Defense Matrix)倡議者Sounil Yu所指出，近期英國部分醫院因病理學暨診斷服務供應商Synnovis遭到勒索軟體攻擊而被迫中斷服務，以及微軟CrowdStrike事件中傳出臺大醫院及臺北榮總之掛號及領藥作業受到輕微影響[3]，除凸顯各醫療院所積極導入雲端服務所可能衍生之風險外，也凸顯強化事中應變及事後復原的重要性；爰此，衛福部在持續強化事前防堵措施之餘，亦宜持續挹注事中應變及事後復原之資源及措施，例如紅隊演練等，以達成相對平衡之網路防禦矩陣。

1、網路防禦矩陣(CDM，Cyber Defense Matrix)係2016年美國銀行首席資安專家Sounil Yu所提出，其核心概念係以識別、保護、偵測、回應、復原為橫軸，設備、應用程式、網路、資料及人員為縱軸所構成之5*5矩陣，可用於檢視組織中資安管理所涵蓋之面向是否完整，其概念已納入OWASP[4] (Open Web Application Security Project)。而Sounil Yu則在2023臺灣資安大會上

[3] 民視新聞網。113年7月19日。微軟當機「台大醫院也受衝擊」 門急診、住院一度暫停。(https://tw.news.yahoo.com/%E5%BE%AE%E8%BB%9F%E7%95%B6%E6%A9%9F-%E5%8F%B0%E5%A4%A7%E9%86%AB%E9%99%A2%E4%B9%9F%E5%8F%97%E8%A1%9D%E6%93%8A-%E9%96%80%E6%80%A5%E8%A8%BA-%E4%BD%8F%E9%99%A2-%E5%BA%A6%E6%9A%AB%E5%81%9C-082136916.html)

[4] OWASP：是一個開放社群、非營利性組織，全球目前有82個分會，主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。(資料來源：國立中山大學資訊安全暨個人資料保護宣導平台 https://ipss.nsysu.edu.tw/p/406-1061-279004,r4902.php?Lang=zh-tw)

指出，目前所有廠商或產品在回應及復原領域都有不夠充分的通病。

2、據悉[5]，2024年6月3日英國國民保健署(NHS)承包商Synnovis(承包病理學暨診斷服務)傳出遭到勒索軟體攻擊，英國倫敦多家國家健康服務(NHS)醫院的部分服務受到影響，其對醫療體系的衝擊包括各醫療院所無法與Synnovis的伺服器安全連線，以即時取得病患的病理學資料。手術和門診因此窒礙難行，特別是需要參考病患血液檢驗結果的輸血作業，手術和門診紛紛取消，或臨時改期、轉送其他單位。

3、接著在同年7月19日，全球Windows電腦陸續傳出藍色當機(BSoD)[6]現象，影響約850萬臺Windows裝置，據悉係資安業者CrowdStrike更新出錯導致，其中達美航空受嚴重衝擊，超過3,500個航班取消，而國內也傳出臺大醫院及臺北榮總之掛號及領藥作業受到輕微影響。

4、由上開資安事件顯示，資安事件之發生難以避免，是以事中應變及事後復原機制是否完善，在未來將更受重視，以CrowdStrike事件為例，其影響範圍雖大，但機構受影響之嚴重程度不同，其差別除了產品的依賴程度之外，即在於事中應變及事後復原機制是否完善。

5、針對事中應變及事後復原面向，衛福部說明，該部已於稽核查檢項目納入設置備援及備份、訂定備份復原程序、定期執行回復測試等項目，評估醫學中心面對資安事件之韌性，此外，該部於111

[5] 聯合新聞網。113年6月5日。倫敦數家大型醫院遭網攻波及 手術大亂衝擊健保服務。(https://udn.com/news/story/6812/8010459)

[6] Blue Screen of Death，指微軟系統當機所呈現之藍白畫面。

及112年分別在林口長庚及彰化基督教醫院辦理攻防演練，內容嚴謹且立意良善，然而衛福部資訊處李建璋處長亦於本院113年3月26日辦理約詢時坦言「(紅隊演練)沒辦法全面實施，太擾民了，而且也要委外資安公司去設計攻防演習」等語，顯見紅隊演練在實務上不易普及，惟據悉國家實驗研究院及資通安全研究院均有建置攻防演練之場域，建議衛福部除持續鼓勵各醫療院所強化事中應變及事後復原措施之餘，亦可進一步評估與相關單位合作進行攻防驗證及演練可行性。

(五)綜上，部立桃園醫院自109年起所發生之一連串資安事件，業已鑑識查明根因並予以防堵，衛福部及桃園醫院並已進行人員責任檢討及人事調整，就近期資安事件通報情形顯示其管理已有相當改善，衛福部允宜持續督導該院資安管理事宜；而在事前防堵之外，事中應變及事後復原日漸受到重視，近期醫療系統所發生之兩起重大資安事件則更加凸顯其重要性，衛福部雖已辦理相關措施，但調查發現仍有諸多挑戰有待克服，有賴衛福部持續鼓勵並挹注醫療院所強化事中應變及事後復原措施，並評估與其他已建置資安驗證場域之相關機關合作攻防演練事宜。

參、處理辦法：

調查意見一至三，函請衛福部督同所屬確實檢討改進見復。

調查委員：賴鼎銘、蕭自佑、王麗珍