臺北市政府資料治理委員會個資保護組
第 1 次會議紀錄

時間：109 年 12 月 30 日上午 9 時 30 分

地點：本府市政大樓 8 樓東北區審議室

主席：個資保護組袁組長秀慧　　紀錄:董孟妤

出(列)席人員：如簽到單

壹、主席致詞：

首先謝謝各位委員及專家學者來協力第一場個資議題的討論，本府前此從來沒有這樣討論過相關個資跟數位治理的方法，所以今天等於是摸著石頭過河，大家有什麼意見都歡迎不吝提供，謝謝大家。

貳、報告事項：洽悉。

參、討論事項：教育局擬設置本市「學生健康管理資訊系統」一案，提請討論

(發言紀要詳後附)

決議：

一、原則上同意教育局用數位雲端化的方式建置系統，但主體上應明確區分教育局作為主管機關及學校作為個資蒐用主體之不同，二者間之權利義務亦應明確區分，亦即個資由學校蒐用，系統放在本府，教育局僅能取得去識別化之統計資料。

二、請教育局依會議決議及委員建議修正提案內容，並提臺北市政府資料治理委員會審議。

肆、臨時動議：無。

伍、散會:上午 11 時 35 分。

臺北市政府資料治理委員會個資保護組第 1 次會議討論事項發言紀要

一、各列席機關：

(一)教育局：

1、本局目前針對學生健康資料的角色，係每年依據學校衛生法作健康促進教育，統整平均比率(例如：齲齒率等等)來告知學校應加強何種事項；亦即，從地方主管機關的高度，就臺北市整體健康狀況提醒各校，每年應以健康促進六大議題之何者為主。其次是作為本市學校與教育部之間的聯繫窗口，例如教育部每年會要求資料上載及資料的準確度，即透過本局向學校宣達。

2、本案「學生健康管理資訊系統」(下稱本案系統)之建置目的有二：第一，硬體介面統一，期望達到程序簡化及效率提升；第二，擴大資料後端運用。至於精準服務部分，我們目前主要目標是強化「教育」，找出需要投注更多時間的教育對象，尚未規劃延伸至個案醫療。

3、有關舊有學生健檢資料轉檔，系統可能可以設計這個功能，讓學校的資料可以完整數位化。另外，本市學生如從國小升學到國中，目前健檢資料是並未隨同移往升學後之學校。

(二)臺北市立聯合醫院：聯醫目前是接受教育局行政委託，辦理國小至高中階段的學生健檢。在健檢

結果上，國中、小學因為沒有抽血，只有一般身體檢查加上蟯蟲及尿液的檢查，結果如有異常，聯醫會跟校護回報，由校護作後續的追蹤。在高中學生部分，因為有血液生化檢查，所以聯醫會出示學生檢查的紙本報告，回報給校護，至於後續的治療及追蹤，則依學生、家長意願自行選擇。

(三)研考會葛主任秘書皇濱：

1、研考會補充說明本案政策的研議重點是：目前教育部向學校蒐集學生健檢資料，本府教育局則否，如果中央有這種蒐集行為，地方政府可否比照辦理？地方政府真的蒐集之後，後續如何運用？至於蒐集後是否用於精準服務，在未來是可能思考的選項，但不在目前規劃範圍。

2、如果只是現有流程的數位化，將各學校的學生健檢資料集中放在本府虛擬的資料庫，現行法律架構似乎就可以處理。建議教育局將本案區分為淺水區與深水區，在提計畫時分層進行法律論述。

二、府內委員：

(一)陳委員素慧(教育局代表)：本案係教育局審酌並非每間學校都有能力數位化，所以由教育局統一協助辦理；又因資安考量，日後系統主機將放在本府機房。如果未來確定要建置本案系統，因主體還是學校，教育局將召開學校衛生委員會，確定各個學校都同意建置後才開始進行。

(二)紀委員嘉真(政風處代表)：

1、本案有兩個主要問題：第一，教育局有沒有資格蒐集學生健檢資料？第二，如果教育局可以蒐集，其後加值運用的範圍可以到哪裡？有關第一個問題，學校衛生法第 2 條、第 3 條都有提到，主管機關是地方政府，那教育局是學校的主管機關，所以從學校衛生法來看，學校堪比教育局的手足，教育局能否以主管機關的立場來蒐集，是否有討論的空間。問題二部分，依照教育局的規劃，本案系統只是作為未來研擬學生健康醫療政策的參考，依學校衛生法第 9 條規定，要經過家長同意才能取得，這個程序一定要踐行。

2、對於政風單位而言，比較擔心的是後續這些資料的處理，不得無故洩漏。另外，如果教育局將資料委外研究，資料要提供到什麼程度？在加值應用前應一併思考去識別化問題。

三、府外委員：

(一)余委員若凡：

1、建立本案系統的目的是什麼？假設現在要比較保守的做，只做統計這件事情，那牽涉到個資的部分，問題可能比較小一點；反之，當我們講到精準行政或是客製化服務這部分，牽涉的問題就很多。

2、有幾個細項需要先釐清：第一，教育局的角色是什麼？本案系統的規劃是「教育局建置資料庫」並要求學校上傳資料，還是學校「把資料留存在由教育局維運的數位化系統」？兩者主、客不同，在個資法上也會面臨不同問題。第二，誰可以接觸到什麼樣的資料？A 校上傳學生健檢資料到本案系統，雖然這個資料庫是建置在教育局裡面，但教育局只是一個代保管的狀態，原則上只有學校可以接觸到這些資料，教育局則否；A 校以外的 B 校，原則上也不能接觸到 A 校的資料。第三，從學校衛生法來看，教育局只是一個諮詢指導的角色，或許在立法的時候還沒有考慮到數位時代需求，但依相關法令，教育局還能以何種方式做到什麼事？也是需要釐清的。

3、針對精準行政部分，如取得同意，比較不會遭遇太大的法令面問題，關鍵是後續怎麼執行。揆諸實際，教育局一般不是客製化醫療服務的執行者，而是要跟醫療院所配合，則醫療院所在其中宜如何取得相關醫療資訊，及扮演何種角色？就現況而言，學校只是委託醫療院所去做健檢，醫療院所出具報告，再由學校轉給家長，後續的治療行為是由家長決定，所以醫療院所的報告僅具參考價值。如果要進一步規劃精準行政，要做到何種程度？假設學生有蛀

牙，是不是醫療院所可以主動通知其進行檢查？均值得思考。

4、本案系統是否曾考慮讓學生或學生家長下載資料？如有，在流程上應有所規劃。例如：學生可不可以轉學籍？得否拒絕繼續將資料留在學校或本案系統中？或許在系統作業流程設計上，可提供更多樣化的選擇及互動介面，俾其知悉曾經給出何種資料、資料現況，以利其更改，及何時可刪除或移往何處。

5、關於同意權行使之主體問題，原則上應由資料主體自己決定。但針對未成年人，到底是家長還是學生自己決定？考量市府轄管的學生大部分都是未成年人，還是建議由家長來作最後的決定。至於非屬個資部分，例如經去識別化，我想沒有太多問題，只是應限制與其他資料庫進行結合。

6、最後，我想政府機關這邊都會有個資安全維護計畫，這部分非常重要，建議本案系統建立以後，這些相關的計畫都要考慮在內，例如資料外洩之事故處理機制等。

(二)王委員琍瑩：

1、先簡單討論一下淡水區的事項。剛剛講到學校在蒐集學生健檢資料的時候的格式問題，我是覺得如果 offline 已經有這些資料，要把它 online 應該沒有問題。如果認為上傳雲端伺服

器很難切割，那可能是技術問題，亦即，如果一定要統一格式跟介面，可能接下來的討論會不容許我們不切割，但我覺得數位化應該是沒有問題，而且可以支持。另關於學校處理這些資料的方式，如果能夠數位化便利輸出、入，併同學籍移轉也都是既有法規、既有紙本都在做的事，那數位化應該也是沒有問題。

2、深水區的事項，首要就是建置資料庫的需求是否存在。就我的了解，不管是臺灣的個資法或是外國的立法例，先進法制在看個資的利用，一直是強調三大重點：第一個重點是最小限度蒐集個資，第二個重點是最大程度的賦權予資料當事人，第三個重點是作最透明的處理機制；不管是家長同意、本人同意，還是成年、未成年之類的同意機制設計，我覺得在確實地、很透明地揭露處理方式、需求及目的之前提下，制度上都可以做得到。但問題在於，要確實、透明地執行揭露，還是要回到最小限度蒐集個資的原則，以及蒐集與處理的目的到底是什麼，因為目的明確後，民眾才會有感，也才會作出有意義的同意。

3、歸納一下本案系統目前可能的建置目的，大概有二：其一是精準行政，其二是公衛政策的規劃。如果是運用去識別化的統計資料，進行健康促進、齲齒、體重等統計分析，例如醫材用了多少、小學學生的體重是不是低於外縣市的

平均值等，因為已經不是敏感個資的利用，本來就可以做。反之，如果是為了精準行政，對應到行銷領域，精準行銷講的就是個人化、客製化行銷，在行政目的上應該也是會這樣，高度可能涉及敏感的個人資料。研考會主秘雖然表示這可能是在未來長期才會發生，但回到前述最小限度蒐集個資原則，如果「目前沒有」這個需求，我們要用什麼理由來承認建置資料庫是必要的？如果是單純公衛政策的需求，透過去識別化資料已經可以做到了，是否還有蒐集這些非匿名化個資的需要？再者，數據數位化之後就會變得比較好用，使用需求也會逐漸增加；本案討論範圍雖以教育局為主，將來會不會認為某些議題確實是有施政需求的，進一部將資料延伸使用到民政、警政、財政及市民公衛系統等領域？因此，關於資料庫的建置目的，仍需要更深入討論，再回來確定相關處理機制是否能讓民眾安心。

4、賴委員有提到，市府方面相當於一個伺服器代管，可是依照法規，我們還是區分「data controller」或「data processor」；processor的責任，包括李董事長提到資安跟加密的問題，即使只提供伺服器代管的服務，還是具有服務提供者的權責。大家可能都了解，現在民眾對 google、Amazon 的信任是大於對政府的信任，所以即使是規劃為代管模式，是否需更保

守地去釐清確認整個處理機制？可以進一步思考。

5、關於統計目的下的去識別化問題，應視個案母數而定。例如：一個偏遠鄉鎮的村落可能有三個人得愛滋病，但整個村落只有十個人，可能輕易地識別出那三個人是誰，所以這可能要看議題來討論。

6、最後，有必要澄清一下資料保存年限與資料可攜、資料被遺忘權是兩回事。在保存年限內，最大程度要賦權給民眾，他的刪除權、可攜權是民眾來決定。那保存年限要多久才算合理？我覺得還是要回歸蒐用目的進行判斷，如果目的是學生「在校時」我們要照顧他的健康，那保存年限設定為畢業之前，應屬妥適。

(三)曾委員韵：

1、學校留存學生健檢資料的現行做法是紙本，如果只是把它數位化，應該是沒有法律面的問題。重點是未來我們要建置這統一的資料庫，造成後面剛剛講的深水區的這些問題。我個人的觀點是，這系統一定要做；如果因為未來長期我們可能會想做到完整蒐集，而導致現在躊躇不前，可以換個角度看看能不能加速一點。

2、本案系統架構一定可以根據我們當前的狀況做出調整。各個學校依法令已經在蒐集學生詳細的健檢資料，我們只是把它數位化；資料的擁

有者是學校，教育局也許只是一個資料的保管者，無法觸碰到這些資料，那現行架構的數位化，應該就只是數位化。就此以觀，現行學校本來就會送資料上來，我們只是透過資訊系統讓他標準化，那只要在技術上對廠商要求：第一是每一個學校都是標準介面，但他的資料是分隔的；第二是依照現行結構，就如同家長同意書所述，學校只能對外提供去識別化的統計的資料，那我們就依照這架構繼續設計資訊系統。進一步言，如果學校要從資料裡面提取教育局想看到的資料，那就只能擷取去識別化的資料，並未脫離前述單純數位化的政策目的。此外，未來如教育局擬蒐用詳細的學生健檢資料，最終的解決辦法就是取得同意；「同意」應區分成兩塊，以目前現行結構來講，學校單獨去跟學生或學生家長取得同意，這件事本來就已經在既有架構內完成了，所以我個人的看法是，教育局要單獨一份同意書，但終究是特殊狀況下才需提取。總之，先數位化，下一步是當教育局要再單獨蒐集個人資料的時候，應另行取得同意，再一併解決其他法律層面問題。

3、如果是確定要數位化，建議功能介面要讓學生家長也可以看到小孩狀況，而不是只有學校有這些資訊。

4、關於教育局在本案系統的角色，我建議的方式是，教育局這邊只有統計資料，但是統計完以

後如果發現特定學生群體有一些特性，可以反過來在系統上設定，將符合特定狀況的學生回饋給學校，那些名單在學校端自然會顯示出來，接續由學校端處理。質言之，系統可以有統計資料可以去做分析，分析完以後把結果反饋給學校，各個學校在自己那端就可以看到詳細的學生資料，再個別去跟家長處理，應屬妥適。

5、另關於本案系統內資料的保存年限，我個人是傾向透過告知機制，讓學生或家長有選擇權。設定保存年限，可使資料不會被立刻刪除，但最終當事人可以自己就資料去留做決定。

(四)賴委員文智:

1、依現行學校衛生法之規定，教育主管機關與學校有各自不同的任務，解釋上不能僅以教育局是學校的主管機關，逕認學校要辦理的事情等同於教育局要辦理的事情。例如該法第 4 條規定，各級主管機關應指定專責單位，這就是主管機關的問題；第 6 條或第 9 條之主體則明定為學校，尚不能一概而論。

2、本案系統的資料蒐用關係中，學校是直接蒐集的主體；可能產生的間接蒐集情形，是學校向學生蒐集後，把它向學生蒐集來的資料交給教育局，這是教育局透過學校間接蒐集；而不論

直接蒐集或間接蒐集，要履踐的要件其實是一樣的。

3、本案教育局要做的事情，在不動現行法規的架構下，只作數位化、只提供雲端服務、只提供資訊工具給學校，其實都做得到。統計性的資訊，教育局在拿到的時候根本不需要知道個別的學生是誰，所以依現行法規架構，完全可以只走淺水的區域，不需要進到深水區即可完成。導致迷思的可能是「資料庫」這個用語，規劃草案其實寫得很好，我們要做的是臺北市學生健康管理資訊系統；要做資訊管理系統不見得要做資料庫，因為做資訊系統只是後面銜接雲端服務，把它描述成資料庫，好像教育局可以接觸到所有資料，但我個人認為未必如此。教育局需要的其實是統計性資訊，我們要做的只有一件事，就是將主體都定位為學校，教育局可以要求學校提供表單，因為所有資料都在這個資訊系統，所以資訊系統可以自動產出教育局需要的表單，這些表單都沒有個人資訊，學校也不需要個別統計才丟出來；只要學校上系統好好 key in，教育局要求的統計性資訊，全部都會由學校按一個鈕送出，送出的全部都沒有個人資料的資料；系統操作的主體是學校，教育局只是背後提供服務的機關，而且教育局作為主管機關跟學校要統計性資料，也完全符合剛剛講到那些法令的規定。

4、進一步言，個別學校做不到的事情，由教育局來做。假設隔壁學校已經有水痘了，教育局從統計性資訊就會發現這些事，就可以發給各個學校，然後由學校提醒家長或學生，鄰近區域已經出現水痘疫情，請家長或學生注意等等。要做到精準行政，事實上不需要掌握資料在教育局手上；教育局跟學校各自扮演自己的工作，其實事情就搞定了。我個人認為，如果純粹把本案系統當作資訊化、數位化、雲端化，那這些資料不會因為他集中在教育局的伺服器上就變成教育局的資料。我們就很像是google、Amazon 一樣，我們提供的是雲端服務、是工具，可是這些資料在系統設計上，教育局是不能接觸到的；教育局只能從學校提供的統計性資料去彙整比對，再把行政所需資訊回饋到學校，讓學校去做所謂精準行政。是以，在整體架構規劃上，只要把資訊系統的操作主體換成是學校、教育局只拿沒有個人資料的統計性數據，僅需學校端多一個提交的動作，就可以把間接蒐集的問題處理掉，因為至少照過去的解釋，認為去識別化的東西就不是個人資料，就沒有間接蒐集，乃至於後續取得同意的問題。

5、我們現在想到的，好像都是全新的資料 key 進來，但有沒有考慮過舊系統資料轉換的問題？因為過去是由學校個別作業，這部分在系統規

劃可能要跟各個學校商量一下。又學生從國小畢業後，其資料是否會帶到國中去？這涉及所謂「學校」的概念界定。例如，某生國小就讀 A 國小，國中就讀 B 國中，B 國中可以蒐集該生的健檢資料，但能否直接將 A 國小的資料移轉到 B 國中？此部分宜由教育局釐清。

6、有關本案系統的資安規劃及系統要求一事，因教育局是資料擁有者，與該局只是提供伺服器給學校使用，二種角色不同，所以二者的資安規劃及系統要求也應有所不同。這部分可能無法照教育局原有規劃辦理，該局應重新檢視。具體而言，資料放在學校跟資料集中在一起，其風險完全不同；當資料散落在各個學校時，如果沒有特定目的，我可能也不會想去看，但是當資料大量集中的時候，縱使沒有特定目的，我可能也會想要進去看一看。個人認為，如果教育局可以接受單純走數位化、雲端化的辦理方向，那整個設計結構及委外規劃，都會跟目前資料呈現出不同樣貌。

7、最後，關於本案系統資料保存期限，我的建議是回到法規，區分成 2 個狀況：其一，紙本部分，學校應訂一個期限，在學生畢業或是學籍移出去之後一定期限刪除；其二，未來數位資料這塊，系統給學生或家長 1 個帳號，讓有權同意者決定數位資料是否繼續留存在系統上。

四、專家學者：

(一)MyData Taiwan 鐘秘書長婉嘉：電子化是必要的，我們先從目前能做、簡單的事情來做，未來如果有其他需求，複雜的問題可以再來討論。我自己覺得比較重要的是本案系統內的資料，什麼時候會被刪掉？學生能否主張將其資料刪掉？是不是學生應該有權利知悉其哪些資料被蒐集了，及有無權利要求刪除？因為學生畢業後，學校對其義務就結束了，所以我建議，畢業時可以給學生一個選擇權，選擇資料保留或刪除，並於系統設計一個通知的機制，跳出通知讓學生去選擇、回復是刪除或同意保留。

(二)開放文化基金會李董事長柏鋒：

1、法律上規定學生健檢資料的蒐集主體是學校，因牽涉到特種個資，縱使是取得同意了，教育局也不該蒐集。雖然北市法務局剛剛從法律找了一些例外規定，但我個人還是覺得應該從嚴解釋，所以特種個資不要同意就隨便轉傳到市府。

2、當然，學校的資料庫還是可以放在市政府裡面，那市政府就要整個負責他的資安。我擔心的是大家都說技術問題可以技術解決，我覺得還是要小心一點，規劃要規劃好一點，因為教育局的招標資料完全沒提到如何切割資料庫及底層是否加密等，可能還是要想一下。而且如果全

系統外包，外包廠商還是會有一個 root 的權限，可以看到全部的資料。雖然資料庫集中化好處理，但是我們一定會面對一些挑戰，所以加密是第一步，第二步就是廠商權限應該如何限制。

3、統計數據跟去識別化資料不同，但依教育局提供的資料看不出來目前這個系統對去識別化的定義。如果教育局發一個公文來索取學校的統計數據，例如：教育局需要 A 校學生的平均身高，這聽起來非常合理，但問題是教育局可以拿到什麼樣的統計資料？這可能需要有人去監督。那對應到市府隱私的主管機關是誰？誰能夠去監督這個程式要怎麼寫，才不會去侵犯到個人隱私？又，如果是統計的話，還要注意最小統計區的概念；這部分可以寫一個程式，讓管理機關去決定統計者可以拿到多少資料。因為涉及特種個資，建議先保守一點；精準資料的使用還是在學校跟家長，而不是教育局。

4、個人資料刪除權跟個人調閱資料權，可能現階段就要考慮，因為個資法本來就規定查詢、更正、刪除是最基本的權利，一定是一開始設計就要考慮到。另一個重要問題是，學生有沒有拒絕我的資料被數位化的權利？個資法目前沒有規定，但國外慢慢有這個趨勢，我連被數位化都可以不要，然後一旦個人可以拒絕，統計資料可能就會有問題；此時，市府在調資料的

時候要怎麼註記有人被刪掉了？會不會影響統計的準確？可能都要考慮進去。

5、最後，關於個人資料刪除權、更正權之行使，不一定要直接給民眾刪除，但至少要提供一個機制。例如：在同意書上直接載明「我(家長)可以透過學校去刪除我的資料」。至於資料是不是畢業後預設刪除，大家可以再考慮一下；我是建議先保守一點預設刪除，再宣導、鼓勵大家同意把資料留下來做科研研究。

(三)**開放文化基金會鄭專員婷宇**：我現在的工作是跟資安社群比較相關，常接觸到資料忽略加密，導致大家都看的到，沒有照顧到個資隱私權，另外就我個人觀點，會想知道資料會保存在機關多久？

五、主席結論：

(一)原則上同意教育局用數位雲端化的方式建置系統，但主體上應明確區分教育局作為主管機關及學校作為個資蒐用主體之不同，二者間之權利義務亦應明確區分，亦即個資由學校蒐用，系統放在本府，教育局僅能取得去識別化之統計資料。

(二)請教育局依會議決議及委員建議修正提案內容，並提臺北市政府資料治理委員會審議。