



醫健通

ehealth

香港特別行政區政府 HKSAR GOVT

電子健康記錄互通的
法律、私隱及保安框架
公眾諮詢文件

互通醫健記錄 延續優質醫護



香港特別行政區政府
食物及衛生局



互通醫健記錄 延續優質醫護

電子健康記錄互通的
法律、私隱及保安框架
公眾諮詢文件

香港特別行政區政府
食物及衛生局
二零一一年十二月



諮詢文件摘要

電子健康記錄計劃

政府建議建立的電子健康記錄互通系統，是要作為本港醫療系統的主要基礎設施，用以提高為本港人口提供醫療服務的質素及效率。這項建議是二零零八年三月發表的醫療改革諮詢文件《掌握健康 掌握人生》所提出的醫療改革建議之一。

2. 這項建議在二零零八年進行的醫療改革諮詢獲得市民普遍支持，食物及衛生局遂於二零零九年實施由政府主導的電子健康記錄計劃，並在局內設立專責的電子健康記錄統籌處，負責籌劃和監督本港電子健康記錄互通系統的發展事宜，確保互通系統在公私營界別得以連貫發展。

- **何謂電子健康記錄互通？** 電子健康記錄是以電子方式儲存的記錄，內載有與個人健康有關的資料。醫療服務提供者取得當事人的同意後，可取覽與該人健康有關的資料作其醫護用途。電子健康記錄互通系統提供一個具效率的平台，讓醫療服務提供者上載和取覽與個人健康有關的資料。
- **為何要推行電子健康記錄互通？** 電子健康記錄互通系統提供重要的醫療基礎設施，讓醫療服務提供者取覽病人健康方面的重要資料，從而提供連貫的優質醫療服務，加強不同醫療服務提供者(例如醫生和醫院)之間的相互配合，使病人獲得更適時的治療及診斷，以及減省重複化驗及蒐集資料的程序。
- **電子健康記錄互通如何推行？** 政府於二零零九年實施電子健康記錄計劃，借助醫院管理局(醫管局)的系統及專業知識，並採用經試驗計劃驗證的**元件組砌方式**，以及公開、預設及共通的技術標準及程序，開發以**病人為本**的電子健康記錄互通系統，供病人**自願參與**。



3. 第一階段電子健康記錄計劃的目標，是在二零一三至一四年度建立電子健康記錄互通平台，連接所有公立醫院和私家醫院，以及確保市場上能夠為私家醫生、診所及其他醫療服務提供者，提供連接至電子健康記錄互通平台的電子醫療記錄/電子病歷記錄系統¹。

電子健康記錄互通的目標

4. 電子健康記錄互通系統的目標如下—

- (a) **改善醫療服務的效率和質素**：醫療服務提供者能夠適時查閱病人的全面醫療資料，並因能夠盡量減少重複檢驗而提升成本效益。
- (b) **促進護理服務的連貫性和配合**：醫療服務提供者可查閱病人的終身健康記錄，以便提供整全護理，並有助在不同醫療層面之間轉介病人和跟進病人個案。
- (c) **加強疾病監察**：可容許迅速地提供資料，以使用於疾病監察，以及利便編製健康統計數據，支援政策制訂和進行公共衛生研究。
- (d) **解決公私營醫療失衡**：促進其他方面的公私營醫療協作，以及在個人層面，讓病人可在公私營服務之間自由選擇而毋須顧慮病歷轉移問題。

¹ 電子醫療記錄/電子病歷記錄系統是由個別醫療服務提供者裝置的資訊系統，用以儲存病人的醫療記錄作本身的醫療用途。這些系統並非自動或必然具備互通功能。要互通電子健康記錄，這些系統必須符合進行互通和連接互通平台的既定標準及程序，而這些標準及程序則是根據與其他規格相若的電子醫療記錄/電子病歷記錄系統進行互相連接而設定的標準及程序來訂定的。



需要制訂私隱及保安框架

5. 我們推行電子健康記錄計劃，對於資料私隱和系統保安極為重視。我們計劃為電子健康記錄互通系統制訂框架，以便在互通系統正式投入運作之前，為資料私隱和系統保安提供法律保障。要建立市民對互通系統的信心和達致電子健康記錄互通的目標，這是必需而不可或缺的。現時，《個人資料(私隱)條例》(第486章)(《私隱條例》)已就個人資料私隱訂定了一般保障措施，適用於所有不同界別。基於病人健康資料的性質，以及醫療服務提供者之間互通醫療記錄的需要，我們認同有必要為電子健康記錄互通系統加入特定及/或額外的私隱及保安保障措施。我們亦認為有必要訂立專門規管電子健康記錄互通的法例，與《私隱條例》相輔相成，同時清楚訂明電子健康記錄互通系統的運作規則。

6. 為此，我們就電子健康記錄互通制訂立法原則和法律、私隱及保安框架(框架)，當中我們參考過《私隱條例》的條文、現行的臨床實務及專業守則，以及海外國家(例如澳洲、加拿大及英國)在健康資料方面的立法經驗，並諮詢公私營界別的相關持份者，包括個人資料私隱專員公署(私隱專員公署)、消費者委員會、多個醫護專業人員團體、病人組織、資訊科技專業人士、醫管局和衛生署。本文件載述了我們就框架所提出的建議，以進一步徵詢公眾和持份者的意見。

主要理念及原則

7. 有關電子健康記錄互通系統的資料私隱和系統保安的主要理念及原則如下—

- **自願參加**(「促使而非強制性」)：只有在**表明和知情同意**的情況下而選擇參加計劃的**病人**，其健康資料才會透過電子健康記錄互通系統進行互通；只有**參加計劃並遵從**電子健康記錄互通規定的**醫療服務提供者**，才可透過電子健康記錄互通系統**上載和取覽資料**。



諮詢文件摘要

- 「病人正接受其護理」及「有需要知道」：醫療服務提供者只可在病人同意下，取覽他們正提供護理服務的病人的健康資料，以及只可取覽為這些病人提供護理服務時有需要閱覽的健康資料；醫療服務提供者取用電子健康記錄互通系統，須受法例規管，確保各項規定均予遵從。
- 預設的電子健康記錄互通範圍：只有屬於電子健康記錄互通預設範圍(「電子健康記錄互通範圍」)內的健康資料，在獲得病人給予同意後，可供其他醫療服務提供者透過電子健康記錄互通系統取覽。至於電子健康記錄互通範圍以外的資料，**不會**透過系統互通。
- 病人身份的識辨和認證：病人的身份會透過中央**個人資料總索引**進行識辨，以確保醫療服務提供者透過電子健康記錄互通系統所取覽的健康資料，確實屬於有關病人，而系統會在病人給予同意或授權時認證病人的身份。已撤回同意的病人，其資料會予「凍結」，不能取覽。
- 醫療服務提供者及醫護人員身份的識辨和認證：服務提供者的身份會透過核證他們的電子醫療/電子病歷記錄系統或其他方法進行識辨和認證。醫護人員的身份亦會透過中央資料庫進行識辨和認證，以確保他們上載的所有病人資料均確實屬於有關病人，而他們透過電子健康記錄互通系統所進行的所有活動，包括取覽及更改資料，均予以適當記錄。此外，醫護人員取覽病人的健康資料，會按醫護人員的職能設定取覽限制。
- 由政府主導系統的管理和執行：政府會擔當主導的角色，**管理電子健康記錄互通系統的運作和執行必要的保障措施**，首要之務是保障病人的資料私隱和系統的保安，同時達成電子健康記錄互通的目標，提供優質醫療服務。



- **病人私隱和醫療服務提供者的需要**：病人的資料私隱須受保障，醫療服務提供者取覽和互通病人健康資料以提供醫療服務則屬**臨床需要**，電子健康記錄互通系統應在這兩者之間取得合理平衡，同時又能保持醫療服務的專業水平。
- **靈活變通和科技中立**：保障電子健康記錄互通系統的資料私隱和系統保安的法律框架，應屬靈活變通和科技中立，以便能配合醫療資訊科技的未來發展。我們會制訂實務守則，用以規管電子健康記錄互通系統的運作。

私隱及保安的法律框架

8. 我們以上述的主要理念及原則為基礎，經考慮各持份者的意見後，為有關的框架制訂了詳細建議，並載於本文件內。現於下文各段扼述這些建議的要點。

電子健康記錄互通的基本模式

9. 病人參與電子健康記錄互通，**純屬自願性質**。下文所闡述的是框架下經簡化後的電子健康記錄互通基本模式，當中反映了醫療服務提供者的臨床需要主導了互通健康記錄資料這點，以及「病人正接受其護理」及「有需要知道」的原則、醫療服務提供者取用互通系統受到規管和其他有關使用電子健康記錄的管制。

「**服務提供者B**可透過**電子健康記錄互通系統**，取覽**服務提供者A**輸入**病人P**的一項健康資料，唯須符合下列所有條件－

- (1) **病人P**給予**表明和知情的同意**，參加了電子健康記錄互通系統。
- (2) **服務提供者A**和**服務提供者B**均參加了電子健康記錄互通系統，並在取用互通系統方面**受到規管**。



- (3) **病人P**的該項健康資料屬於**電子健康記錄互通範圍**，可經由電子健康記錄互通系統互通。
- (4) **服務提供者A**取得**病人P**的**同意**(見下文「病人的同意」一節)，以便把**病人P**的健康資料上載到電子健康記錄互通系統。
- (5) **服務提供者B**取得**病人P**的**同意**(包括轉介)，以便取覽**病人P**在電子健康記錄互通系統的健康資料。
- (6) **服務提供者B**需要取覽和使用**病人P**的該項健康資料，以便向**病人P**提供專業醫療服務。
- (7) 所有有關各方的身份均經**獨特的識辨和認證**，而所有上述事項/活動均**記錄**於電子健康記錄互通系統。
- (8) **系統設有保安措施**，確保只有上述條件符合才能取覽該項健康資料。」

10. 我們基本上是透過改進這個經簡化的基本模式來制訂框架，當中考慮到存取和使用電子健康記錄互通系統的實際情況。我們只有在理據充分的情況下，並考慮到有關情況或現行做法後，才建議偏離這個模式和容許例外處理。現於下列各節闡述這個模式的各個方面。



病人的同意

11. 病人參加計劃，是建基於其給予**表明和知情的同意**。實際上，為協助病人在知情的情況下作出決定，我們會向病人提供有關資料，當中包括：電子健康記錄互通的範圍、目的及使用；病人的權利；私隱及保安的保障；以及退出安排等。本文件提出了一些具體建議，以利便病人給予同意，讓服務提供者取覽其資料－

- (a) 病人可以兩種形式給予同意，讓醫療服務提供者取覽/上載其電子健康記錄資料：(i)設有一年時限的滾續同意，由該醫療服務提供者最後一次向病人提供護理的日期起計一年後，有關同意便告失效；(ii)不設時限的同意，這類同意會一直維持有效，直至病人表明撤銷其同意為止。
- (b) 被認為無能力自行給予知情同意的病人、年齡在16歲以下的未成年人和精神上無行為能力的人，當局會為他們作出特別安排，由代決人代為同意。
- (c) 鑑於醫管局和衛生署備存提供醫療服務所必需的健康記錄，病人如選擇參加電子健康記錄互通，便須在登記時同時給予醫管局及衛生署不設限期的同意，讓他們作為醫療服務提供者可取覽/上載其電子健康記錄。
- (d) 電子健康記錄互通系統會設有功能，方便醫療服務提供者按照現行的轉介做法，互相轉介病人。具體而言，如服務提供者A把病人轉介至服務提供者B接受醫療服務，服務提供者A可指明服務提供者B可取覽病人那一部分的電子健康記錄。
- (e) 容許在特殊情況(例如緊急情況)下可未取得病人事先同意而取覽其電子健康記錄。這類取覽必須符合《私隱條例》的規定，而可由誰人和在何種情況下作出這類取覽，會受到嚴格規管。



12. 病人可在任何時間退出電子健康記錄互通並撤銷所給予的同意。為達致法律和審核方面的目的，我們會訂立安排以便把資料「凍結」，不許取覽，並把有關資料存入舊資料藏庫供保存一段特定時間(見下文有關資料的保存)。病人如在凍結期內選擇再次加入電子健康記錄互通系統，其電子健康資料便可恢復互通，但他們需要再次確認所有先前給予個別醫療服務提供者的同意。病人如在凍結期後才選擇再次加入電子健康記錄互通系統，其先前建立的電子健康記錄資料便不再存在，他們需要和其他新參加系統的人士一樣，重新建立其個人電子健康記錄。

電子健康記錄互通的設定範圍

13. 我們為電子健康記錄互通制訂了建議的資料互通範圍(電子健康記錄互通範圍)。這個範圍已顧及到醫護人員為病人提供醫療服務的臨床需要。我們亦建議分期推行電子健康記錄互通範圍，以配合電子健康記錄互通系統的技術能力，以及醫療服務提供者使用電子健康記錄互通系統的情況。

14. 建議的電子健康記錄資料互通範圍，詳載於本諮詢文件的**附件D**。在電子健康記錄互通的第一個發展階段，範圍會包括下列項目－

- (a) 個人身份和基本資料
- (b) 診症/與服務提供者接觸的資料(摘要)
- (c) 服務提供者之間的轉介
- (d) 不良反應/敏感
- (e) 診斷、醫療程序及用藥
- (f) 防疫注射記錄
- (g) 化驗及放射結果
- (h) 其他檢驗結果



15. 為保持電子健康記錄的完整和齊全，確保向病人提供的醫療服務符合專業標準，原則上醫療服務提供者會根據「病人正接受其護理」和「有需要知道」的原則，以及病人所給予的同意，獲准取覽由其他醫療服務提供者上載並屬電子健康記錄互通範圍內的任何健康資料。除非是依照已述明的原則，透過在電子健康記錄互通系統設定取覽限制的方法而另作規定，否則電子健康記錄互通系統不會容許在電子健康記錄互通範圍內的任何特定健康資料可予隱藏而不許他人取覽，或須取得額外同意才可取覽。參與計劃的醫療服務提供者，須把其病人的電子醫療記錄/電子病歷記錄中屬電子健康記錄互通範圍內的健康資料，上載至電子健康記錄互通系統，不得有所豁免。

電子健康記錄資料的取覽、使用及保存

16. 電子健康記錄互通資料，其主要用途是促進病人護理的連貫性。參與電子健康記錄互通的醫療服務提供者，使用透過電子健康記錄互通系統獲取的資料，必須遵守有關規則的規管。醫療服務提供者原則上不會獲許在任何其他情況下取覽和使用電子健康記錄資料，而且須受審核有否遵守規定。《私隱條例》下有關查閱和使用個人資料的一般豁免會視乎情況而可能適用，但此等應用須受電子健康記錄互通系統營運機構的管制，以確保各項規定均予遵從。

17. 為了公眾衛生的利益着想，電子健康記錄互通系統的資料可用於疾病監察和公共衛生研究，這屬於一項特定豁免，而且須遵從日後所訂立的電子健康記錄法例為這些健康資料用於次要用途所設定的機制。具體而言，電子健康記錄互通系統營運機構會批准使用不能識辨個人身份的資料供作疾病監察和公共衛生研究。然而，使用可識辨個人身份的資料作疾病監察和公共衛生研究，則須事先獲得食物及衛生局局長按研究委員會的建議而給予的批准。



18. 一般而言，只要病人持續參與電子健康記錄互通，其電子健康記錄資料便會一直保存在電子健康記錄互通系統。病人如退出電子健康記錄互通，或已經去世，他們在電子健康記錄互通系統的資料便會「凍結」，並存入舊資料藏庫，不許任何醫療服務提供者取覽。參考各項法例及專業實務，退出病人的資料會繼續保存三年，已故病人的資料則會保存十年。凍結期屆滿後，電子健康記錄系統會移除可識辨身份的資料²，並保留在系統內作次要用途，例如用於上文所述的疾病監察和公共衛生研究。

身份識辨、認證、取覽限制及保安

19. 為確保有關電子健康記錄資料屬於有關病人，以及認證服務提供者的身份以供上載和取覽資料，我們會推行一系列保安措施，並將之納入電子健康記錄互通的擬議實務守則和運作指引內(見下文)。這些保安措施包括一

- (a) **病人身份的識辨和認證**：主要利用香港身份證(智能身份證)與系統的資料進行核證(例如核對香港身份證的稽核數碼)；沒有香港身份證的病人，則使用其他輔助途徑進行身份識辨和身份認證；由電子健康記錄互通系統中央備存的個人資料總索引，會用來對病人的身份進行獨特識辨，以及連結病人的電子健康記錄資料。
- (b) **服務提供者身份的識辨和認證**：醫療服務提供者取用電子健康記錄互通系統，系統會透過核證其電子醫療記錄/電子病歷記錄系統或其他方法認證其身份；電子健康記錄互通系統會透過中央核證來確定健康資料的完整性和來源，而個別醫療服務提供者上載、取覽及更改電子健康記錄互通系統的健康資料，所有這些活動均會加以記錄，以確保所有資料及活動均可確切查悉提供資料和進行有關活動的醫護人員。

² 移除識辨身份的資料是要使電子健康記錄資料不能識辨任何病人的身份。



- (c) **按醫護人員的職能設定取覽限制**：所有連接電子健康記錄互通系統的電子醫療記錄/電子病歷記錄系統，須按醫護人員的職能設定取覽限制。換言之，不同職能的醫護人員，其電子醫療記錄/電子病歷記錄會獲給予不同層級的取覽權力，以取覽不同的資料和使用系統的不同功能(例如只有醫生才可上載藥物處方，但護士就不可以)，從而得以上載和取覽電子健康記錄互通系統的資料。電子健康記錄互通系統會根據一個醫護人員中央登記資料庫進一步核對醫護人員的資料取覽。透過電子醫療記錄/電子病歷記錄系統取用互通系統的活動，均會保存記錄，並須接受審核和檢查。
- (d) **整個系統的保安措施**：存於電子健康記錄互通系統內的資料庫、檔案、舊資料藏庫的一切相關資料，以及在電子健康記錄互通系統與個別電子醫療記錄/電子病歷記錄系統之間互相傳輸中的所有資料，均予以高度的保安加密；從電子健康記錄互通系統下載電子健康記錄資料，將限於個人資料總索引所載的資料和有關藥物敏感的資料，以盡量減少風險；與病人相關的電子健康記錄系統活動(例如在其電子健康記錄遭人取覽時)，系統會透過電子方式(如短訊服務或電郵)向病人發出警示；個別電子醫療記錄/電子病歷記錄系統亦須採取保安措施，並遵從實務守則及運作指引的規定，確保使用者一端的保安。

病人查閱和改正資料

20. 與《私隱條例》的規定一致，病人作為資料當事人，可提出查閱資料要求，但須繳付指定的費用。然而，我們建議日後的電子健康記錄法例在查閱資料要求方面，應採用比現行的《私隱條例》更為嚴格的標準，規定查閱資料要求必須由當事病人自己或其代決人(例如未成年人的父母及精神上無行為能力的人的監護人等)提出，任何其他第三者即使獲病人授權，亦不得提出。這項規定是要確保更高的資料私隱水平，以及確保除了已獲當事病人給予同意的醫療服務提供者外，只有該病人本身可以直接查閱其健康資料，而非可由任何其他第三者代其查閱。



21. 在電子健康記錄互通系統下，提供病人健康資料的醫療服務提供者可按照現行臨床實務的做法，主動或應病人的要求修訂病人的健康資料。為符合《私隱條例》的規定，病人亦可要求改正其電子健康記錄資料，而這類改正電子健康記錄互通系統資料的要求會由負責提供資料的醫療服務提供者處理。服務提供者可改正資料，但如不同意資料有誤，則可拒絕修改，而在這情況下須就此事作出附註。如上文所述，所有這些更改或附註，電子健康記錄互通系統均予以記錄，作為系統的部分保安措施，而任何修改資料將會附連於電子健康記錄，不會取代原有資料。所作的更改或備註亦會予以標示，以便其後取覽電子健康記錄的醫療服務提供者更容易察悉有關資料。為防止有人規避保安措施，凡對病人的個人資料總索引資料進行修改，必須取得當事病人的同意。

實務守則、指引、保安審核、投訴及覆核

22. 在框架下，我們建議制訂一套實務守則，就參與的醫療服務提供者的內部取覽程序和限制，以及電子醫療記錄/電子病歷記錄系統的保安標準及要求，臚列有關的規則及規例。建議的實務守則由電子健康記錄互通系統營運機構發出，對醫療服務提供者具約束力，規定他們的電子醫療記錄/電子病歷記錄系統必須符合實務守則的規定。不遵守實務守則本身並不會直接令有關人士須承擔電子健康記錄法例所訂立的法律責任。然而，實務守則必須獲電子健康記錄法例訂定特定的權力予以支持，以便一旦在覆核投訴及進行保安檢查或審核時發現違反保障資料私隱或系統保安的情況，電子健康記錄互通系統營運機構可要求個別電子醫療記錄/電子病歷記錄系統的使用者及管理人員採取補救行動，以符合實務守則的規定。

23. 我們亦建議電子健康記錄互通系統營運機構可頒布一些並非法定的運作指引、最佳實務指引、程序準則及/或其他形式的指引，訂明電子醫療記錄/電子病歷記錄系統應如何運作和執行，以及如何與電子健康記錄互通系統互聯和取用互通系統。雖然這些指引並非通過法例強制執行，但當電子健康記錄互通系統營運機構需要驗證電子醫療記錄/電子病歷記錄系統是否符合



所需的保安標準，是否適合與電子健康記錄互通系統互聯，又或應否准許醫療服務提供者或其醫護人員取用電子健康記錄互通系統時，可考慮到當中是否有遵從這些指引的規定。制訂指引有助在資料私隱及系統保安方面維持高度的標準；而訂立規則往往有欠靈活，未能配合日新月異的科技發展。

24. 為確保各方遵從規定和作為一項制衡措施，電子健康記錄互通系統營運機構應獲授權對各醫療服務提供者的電子醫療記錄/電子病歷記錄系統和內部取覽限制，進行保安審核。這類檢查或審核可採用抽查方式或因應投訴而進行。我們亦會對電子健康記錄互通系統，以及該系統與個別電子醫療記錄/電子病歷記錄系統之間的互聯定期進行保安審核，以確保其運作安全和保安穩固。除進行保安審核外，電子健康記錄互通系統的技術設計亦會加入一些針對違反保安情況的內置保護功能，透過持續監察系統偵測任何明顯的異常情況，例如頻密取覽大量病人記錄和作出大幅度修改(見下文)。

25. 我們會在日後的電子健康記錄法例下訂立機制，用以就電子健康記錄互通展開覆核和處理投訴。這個機制可讓市民就電子健康記錄資料的取覽及使用、電子健康記錄互通系統本身或與互通系統連接的個別電子醫療記錄/電子病歷記錄系統所涉的資料私隱及系統保安事宜作出投訴，以及讓當局展開覆核。

刑事懲處

26. 為產生阻嚇作用，防止發生違反保障電子健康記錄互通系統資料私隱和系統安全的行為，我們建議特別針對未獲授權並惡意取用電子健康記錄互通系統施加刑事懲處。在訂定懲處級別時，我們會參考其他現行法例條文³針對同類作為所訂立的懲處。醫護人員本着真誠為病人提供醫療服務，在輸入電子健康記錄資料時出現的無心之失，或其他並非蓄意的違規事件，我們不打算就這些情況訂立刑事責任。

³ 《電訊條例》(第106章)第27A條(一經定罪可處罰款2萬元)及《刑事罪行條例》(第200章)第161條(一經循公訴程序定罪可處監禁5年)。



資料私隱及系統保安的技術事宜

27. 為確保在法律和技術方面取得協調，我們必須同時針對本港目前的電子健康資訊的技術和應用，以及日後的電子健康記錄互通系統的資訊科技基建平台的技術設計及運作，考慮法律和保安保障措施。

電子健康記錄互通系統的保安與技術設計

28. 由於電子健康記錄性質敏感，且須存放於互聯網的環境中，我們十分重視電子健康記錄互通系統的保安基礎設施。經審慎考慮後，我們建議採用中央資料庫的方式，而非其他方式(例如以分布式儲存電子健康記錄互通資料)。我們委託顧問進行研究，審訂我們的建議是否有效，所得的結論是這建議方向正確，而且已涵蓋相關的技術事項。醫管局就電子健康記錄核心互通基礎設施(電子健康記錄核心設施)結構設計所採用的原則之一是加入「內置保安系統」，以保障資料保安及病人的私隱。

保安及審核制度

29. 除基礎設施工具外(例如認證及授權、防火牆及入侵偵測工具)，亦應設立全面的保安及審核制度。該制度應涵蓋各個範疇，包括政策、標準、系統設計、核證、問題管理，以及培訓和溝通。具體而言，它會包括為電子健康記錄核心設施和電子醫療記錄/電子病歷記錄系統制訂一套保安政策及程序(例如電子醫療記錄/電子病歷記錄系統須安裝特定保安軟件)；就開發軟件和威脅管理設定保安程序；以及就保安風險評估提出建議，當中會參考本地和海外的經驗。我們在二零一零年年底委託進行有關資訊科技保安及審核制度的顧問研究，確保有關保安的各個方面均經適當檢討和處理。



私隱影響評估及私隱循規審核

30. 為確保電子健康記錄互通系統符合私隱保障標準，我們會根據私隱專員公署所發出的指引進行私隱影響評估⁴及私隱循規審核⁵，以確保各個保障私隱理念均有效落實。為此，我們首先委託進行了一項私隱影響評估範圍界定研究，以審視框架和制訂整體的私隱影響評估策略計劃。

31. 據私隱影響評估範圍界定研究所得的結論，框架符合本港的監管要求，亦與海外的做法相若。該研究亦為一些修訂和澄清提出建議。其後，我們因應顧問研究的結果，對框架作出進一步的改進。

下一步工作

32. 我們現就框架諮詢公眾，你的意見有助電子健康記錄互通系統成功推行。請於**2012年2月11日**或之前，以下列方式提出你對這份諮詢文件的意見。

郵寄： 香港添馬添美道2號
政府總部東翼19樓
食物及衛生局
電子健康記錄統籌處

傳真： (852) 2102 2570

電郵： eHR@fhd.gov.hk

網址： www.ehealth.gov.hk

⁴ 私隱影響評估一般被視為對決策過程有用的系統性風險評估工具。透過這系統性的程序，可評估一項計劃對個人資料私隱的影響，目的是避免或減低不利影響。

⁵ 私隱循規審核旨在：(i)評估和評核個人資料的收集、編整和處理工作，在依從《私隱條例》的規定，特別是依從該條例附表1所載的六項保障資料原則方面，達到何種程度；(ii)識別資料保障系統的潛在弱點；以及(iii)為檢討該系統提出建議。



33. 我們現正同時進行資訊科技基礎設施的設計及開發工作，並會把去年為資訊科技保安及審核制度展開的顧問研究所得的結果納入為考慮因素。我們亦會根據私隱影響評估策略計劃，進行全面的私隱影響評估研究，當中第一階段的研究會聚焦於現時的試驗計劃，即經融合其他試驗計劃(例如長者醫療券的醫健通系統)後進行重整的公私營醫療合作－醫療病歷互聯試驗計劃。私隱影響評估會審視一些上文所建議的資料及私隱保障理念的實施情況。我們考慮公眾諮詢的結果後，會對框架作出改進，並視乎情況把所作的修訂納入私隱影響評估研究的範圍內，以及進行草擬電子健康記錄法例的預備工作。



www.ehealth.gov.hk

香港特別行政區政府
食物及衛生局出版
政府物流服務署印