《電子健康紀錄互通系統條例草案》委員會

政府當局就二零一五年五月十二日會議的事項作出的回應

本文件載述政府當局就電子健康紀錄互通系統(互通系統)條例草案委員會於二零一五年五月十二日會議上所討論事項作出的回應。

(a) 有關第 41(6)條擬議罪行的草擬事宜

2. 根據第 41(6)條，任何人有以下情況，即屬犯罪—

(a) 明知而導致電子健康紀錄所載的資料或資訊(i)被取覽；(ii)被更改；或(iii)的取覽、可靠性、保安或處理受到損害；及

(b) 有下述意圖或目的而導致上述取覽、更改或損害—(i)意圖犯罪(**不論是在該人導致上述取覽、更改或損害的同時犯罪，或是在日後任何時間犯罪**)；(ii)不誠實地意圖欺騙(**不論是在該人導致上述取覽、更改或損害的同時進行欺騙，或是在日後任何時間進行欺騙**)；(iii)目的在於令其本人或他人不誠實地得益(**不論是在該人導致上述取覽、更改或損害的同時得益，或是在日後任何時間得益**)；或(iv)不誠實地意圖導致他人蒙受損失(**不論是在該人導致上述取覽、更改或損害的同時導致他人蒙受損失，或是在日後任何時間導致他人蒙受損失**)。

<u>第 41(6)(b)條的“時間”一詞</u>

3. 在二零一五年五月十二日的會議上，有委員詢問第 41(6)(b)條中的英文文本使用“whether on the same occasion...or on any future occasion”而非“whether at the time…or at a future time”意思上的差別。他也建議檢視相應中文文本“不論是在...的同時...或是在日後任何時間...”的寫法。

4. 我們已進一步研究有關事宜。我們可確認有關的中英文草擬本在法律意思或理解方面並沒有差異。因為中文文本並非英文文本的直譯本(相反亦然)，中文文本會按本身語言的特性及用法去理解。“On the same occasion”這片語在法律上亦不時會使用。該片語為將意圖作出的有關行為給予一種必要的“時空”意味。相比下，若然在英文文本中使用“at the same time”會較使用“on the same occasion”意思上有更多限制。

5. 另一方面，如我們在中文文本中使用“同一事件中”，便可能將會引致比原意涵蓋了更長的時間。我們認為現時的中文文本已經如英文文本般恰當反映出政策目的。此外，《電子健康紀錄互通系統條例草案》(條例草案)的第41(6)(b)條的草擬是使用了與《刑事罪行條例》(第200章)第 161(1)條基本上相同的字眼。其中的考慮是在訂明第 41(6)條的新罪行以針對有關「電子健康紀錄所載的資料或資訊」(相對於一般「電腦」)，及達至不單「取覽」有關的資料或資訊，而是「更改」及「損害取覽、可靠性、保安或處理」也會屬違法時，其所要求的犯罪/不誠實的意圖或目的能保持一致性。由於我們應在檢控有相類元素的個案時保持一致的做法，因此我們認為這種字眼上的一致性是必需的。

第 41(6)(b)條的“any”一詞

6. 有委員在會議上詢問，在第41(6)(b)條的“any future occasion”中，為何會使用“any”，而不是“a”。如上述，條例草案的第41(6)(b)條的草擬是使用了與第200章第161(1)條基本上相同的字眼，而保持這種一致性是必需的。除了這一致性的因素外，我們亦已從語言的角度方面考慮。雖然最新的草擬常規是要避免不加區別地使用“any”，但確實仍在有些情況下使用“any”較“a”或“an”為佳。我們在第41(6)(b)條使用“any future occasion”而並非“a future occasion”，原因是我們想提及*一般*日後的任何時間。如使用“***a*** future occasion”，焦點可能會稍為移至尋找日後*一某特定*的時間。同樣的理據亦在中文文本中適用。

第 41(6)(b)條的整體草擬

7. 有委員亦在會議上觀察到第 41(6)(b)條英文文本的“whether on the same occasion…or on any future occasion”，在中文文本時是在第(i)至(iv)款各款的句尾分別在括號內出現，並詢問有關條文的中文文本草擬能否改動，讓其更易理解/更便於閱讀。如上述，條例草案的第 41(6)(b) 條的草擬是使用了與第 200 章第 161(1)條基本上相同的字眼，而保持這種一致性是必需的。除了這一致性的因素外，中文文本和英文文本為了因應各自的語言特性，使用了不同的句式架構。在本條中，“whether on the same occasion…or on any future occasion”這片語與時間有關，以修飾在第(i)至(iv)款下，各個意圖行動於何時進行。而因為第(i)至(iv)款使用了不同的動詞，為修飾各意圖行動於何時進行，在中文文本中的動詞須緊接其時間，例如“同時犯罪…日後任何時間犯罪”。

(b) 條例草案第 50 條訂明在某些情況下，電子健康紀錄專員可要求交出紀錄或文件

8. 條例草案第50(1)條訂明，電子健康紀錄專員如覺得有情況顯示有第(2)款指明的任何事件發生，可藉書面要求**登記醫護提供者**，交出符合以下說明的紀錄或**文件**—(a)攸關或可能攸關該事件的；及(b)**由該提供者管有的**。

<u>條例草案第 50(1)條有關“文件”的定義</u>

9. 如我們在二零一五年二月二十三日回覆助理法律顧問的函件(立法會 CB(2)911/14-15(01)號文件)內解釋，及隨後在二零一五年五月十二日的會議上詳細說明，《釋義及通則條例》(第 1 章)第 3 條指明，“文件”(“document”)指“任何刊物及以字母、字樣、數字或符號的形式，或以超過一種上述的形式在任何物質上書寫、表達或描述的任何資料”，這有關定義並沒有排除電子形式的文件。而當在某條例中並沒有指明任何定義時，“文件”一詞的理解將會跟隨第 1 章中就該詞的定義。

10. 如在特定的情況下，在第 1 章中就“文件”一詞所界定的意思並未能反映政策的意向，那便有需要為該詞指明定義。在二零一五年五月十二日的會議上，助理法律顧問及一名委員建議我們在條例草案第 50(1) 條中特別表明“文件”一詞涵蓋“電子文件”，以減低造成誤解的風險。就上述考慮而言，及在本條例草案的情況下，我們認為沒有需要在條例草案下界定“文件”一詞。我們仍然認為有關做法是不必要的。

11. 至於助理法律顧問在會議上提及的兩個例子(即是《版權條例》(第 528 章)和《非應邀電子訊息條例》(第 593 章))，我們想指出前者其實並沒有特別就“文件”一詞下定義，而後者則有著與本條例草案不一樣的特定情況，並不適合作為參考。就此而言，委員可留意雖然有《電子交易條例》(第 553 章)是和處理電子交易有關的，但“文件”一詞在該條例中同樣亦沒有作出定義。實際上，在超過 450 條本地法例的搜尋結果中，只有約 20 條條例包含“文件”一詞的定義。有關例子包括《土地註冊條例》(第 128 章) (定義該詞包括“任何地圖、圖則或繪圖”等)、《教育條例》(第 279 章) (定義該詞包括“任何帳目、存根、教科書、練習簿”等)、《公司(清盤及雜項條文)條例》(第 32 章) (定義該詞包括“傳票、通知、命令和其他法律程序文件”等)。從這些例子中，特定為“文件”一詞作出定義是有明確需要的。然而，在本條例草案中我們並未預見任何為該詞訂明特定定義的明顯原因。

條例草案第 50(1)(b)條“由該提供者管有的”的條件

12.　　在會議上，有委員建議我們修改電子健康紀錄專員根據第 50(1)(b)條可要求醫護提供者交出的紀錄或文件的文本。經考慮有關建議後，我們準備提出擬議修訂以擴展範圍至“由該提供者管有或控制的”，有關擬訂已以追蹤修訂形式載於**附件 A**。這些草擬的修訂或因應與律政司討論後再加以完善。

醫院管理局(醫管局)及衞生署

13.　　助理法律顧問及主席也在會議上建議，除了登記醫護提供者，醫管局及衞生署同樣應根據第 50 條，在電子健康紀錄專員的要求下交出紀錄或文件。我們經考慮有關建議後，我們準備提出擬議修訂以達至此效果，有關擬訂已以追蹤修訂形式載於**附件 A**。這些草擬的修訂或因應與律政司討論後再加以完善。

(c) 《實務守則》

14.　　電子健康紀錄專員可根據條例草案第 51 條訂明發出《實務守則》。如之前解釋，《實務守則》乃行政文件，旨在為使用互通系統提供最佳做法指引。《實務守則》屬運作性質，將能幫助使用者更易明白系統的運作及更佳地執行某些功能，如處理註冊申請的程序。醫護提供者並非要強制性跟隨《實務守則》中所有的建議做法，但它們須被提醒不遵守建議做法的風險。

15.　　《實務守則》現正在準備當中，並將因應通過的《電子健康紀錄互通系統條例》的內容、互通系統最終的運作流程，及包括相關的持分者為成員的電子健康紀錄互通督導委員會的意見而訂定，並於互通系統啓用前公布。我們之前已於二零一四年十二月八日的會議上向委員簡介《實務守則》的性質、框架和要點。不過，鑑於委員在二零一五年五月十二日的會議上的要求，我們現將至今的《實務守則》英文版“工作初稿”載於**附件 B** 供委員參考。我們希望委員注意此文件是參考海外有推行電子醫療或病人紀錄系統的機構及著名組織的類似指引，及現已草擬的條文(已考慮我們建議修訂的條文)而準備，內容屬臨時性質草稿，它有助了解將來最終的《實務守則》的內容，而這些內容需要確立條例草案的條文後及進一步諮詢有關持分者後才可以作最後增刪定稿。在待條例草案通過後制訂守則、就守則作出諮詢及發布守則的工作，屬電子

健康紀錄專員的責任。這些責任不會受此“工作初稿”文件所影響。

(d) 投訴處理機制

16. 條例草案第48(h)條訂明，電子健康紀錄專員具有職能去設定機制，以處理關乎互通系統運作的投訴。如我們在二零一五年二月二十三日向助理法律顧問發出的函件(立法會 CB(2)911/14-15(01)號文件)所解釋和在二零一五年五月十二日的會議上詳細說明，我們會參考現時政府當局的相關的指引以設定機制，並在完成後適當地向持分者發布。

17. 助理法律顧問在會議上詢問我們應否在條例草案中載述作出及處理有關互通系統運作的投訴的格式和方式。我們重申這在此條例是不需要的。電子健康紀錄專員的主要工作是營運、維持和發展互通系統，其工作性質與申訴專員、個人資料私隱專員，或監警會等非常不同(處理投訴 / 因應法定/嚴重違規的投訴進行調查是這些機構的其中一項主要職能)。在這方面，電子健康紀錄專員辦事處的情況與很多政府部門、公營機構(例如醫管局和機場管理局)、立法會秘書處等更為相似。它們的主要職能是提供服務、營運系統/設施、管理資源等。這些機構雖然也可能要處理投訴，但相關條例(如有的話)中亦沒有載述作出和處理投訴的格式和方式。

18. 在會議上，有委員查詢有關互通系統運作的處理投訴機制的詳情。我們已經解釋，我們會參考現時政府當局的相關的指引以設定詳細的機制，並在完成後適當地向持分者發布。我們把有關的重要原則及擬議工作流程的草擬框架載於**附件 C** 以供參考。

食物及衞生局
2015 年 5 月

附件 A

有關在某些情況下要求醫護提供者交出紀錄或文件的
擬議修訂

(備註：擬議修訂載於以下條例草案的節錄，以紅色及底線／刪除線標示。)

****

50. 在某些情況下，專員可要求交出紀錄或文件

(1) 專員如覺得有情況顯示有第(2)款指明的任何事件發生，可藉書面要求~~登記~~訂明醫護提供者，交出符合以下說明的紀錄或文件—

(a) 攸關或可能攸關該事件的；及

(b) 由該提供者管有或控制的。

(2) 有關事件是 —

(a) 有關醫護提供者違反 —

(i) 本條例的任何條文；

(ii) 根據第 51 條發出的《實務守則》的任何條文；或

(iii) 有關登記的任何條件；

(b) 有關醫護提供者不再在有關登記所關乎的服務地點，提供醫護服務；

(c) 有關醫護提供者不再符合 —

(i) 專員就連接該提供者與互通系統而指明的規定；或

(ii) 專員就資料互通而指明的系統規定；

(d) 有關醫護提供者的服務或業務的性質，不再與第 26 條指明的資料及資訊的使用目的相符；或

(e) 有關登記可能損害互通系統的保安，或危害其完整性。

(3) 有關要求須指明交出有關紀錄或文件的方式。

****

<u>附件**B**</u>
<u>(</u><u>只有英文版本</u>**<u>)</u>**

Code of Practice for Using eHR for Healthcare (Working Draft)

1. INTRODUCTION

1.1. PRACTCAL GUIDELINES FOR USE OF eHRSS

This Code of Practice (COP) is an administrative document issued by the Commissioner for Electronic Health Record (“the Commissioner” or “eHRC”) under section XX of the Electronic Health Record Sharing System Ordinance (Cap XXX) (eHRSSO) (“the Ordinance”).

This COP helps eHRSS users and participants (in particular healthcare provider’s executive, administrative, technical staff and healthcare professionals) to better understand the operation of and the requirements for using Electronic Health Record Sharing System (eHRSS or the System). It sets out the major principles, standards and best practices for using eHRSS in a secure and proper manner.

This COP is for reference and it is not mandatory to comply with all the requirements and best practices set out in it. HCPs and healthcare professionals may find alternative ways other than those recommended in the COP which also enable them to meet the relevant requirements in the eHRSSO. However, not otherwise engaging in appropriate practices may lead to security or privacy incidents and put the participants at risk of not able to continue to use the system.

Mere non-compliance with this COP by itself does not render the person to any criminal proceeding unless such action of breach in itself constitutes an offence under the eHRSSO or other ordinances.

1.2. TARGET READERS

Section 2 - *COP for eHR Management Executives, Administrative and Technical Staff* provides general and practical guidance for Management Executives, Administrative and Technical Staff working in Healthcare Providers (HCPs) who have participated in the eHRSS. This part highlights the responsibilities of the healthcare staff management, administrative duties and technical set up for using eHRSS.

Section 3 - *COP for eHR Healthcare Professionals* provides general and practical guidance specific for healthcare professional. This part highlights the responsibilities and good practices for healthcare professionals in the use of eHRSS for sharing health information for providing healthcare to Healthcare Recipients (HCRs).

1.3. USE OF COP

Reading this COP facilitates understanding and compliance with the Electronic Health Record Sharing System Ordinance (eHRSSO) and other relevant ordinances to safeguard HCRs' privacy and confidentiality for using eHRSS. In compiling this COP, reference has been made to similar guidelines issued by various authorities and renowned organisations in overseas countries where electronic medical or patient record systems have been implemented.

This COP provides technical and operational guidelines and recommended best practices for participating HCPs and their healthcare staff (HCS). However, it should not be regarded as exhaustive.

Users are recommended to read this COP in conjunction with the eHRSSO (Cap XXX), PD(P)O and other references quoted in this document. Other useful references include notices, newsletters and relevant updated information issued by the eHR Office. Readers are also reminded to make reference to the Code of Practice and Guidance issued by the Office of the Privacy Commissioner for Personal Data (PCPD) regarding protection of personal data privacy.

eHRC may, from to time revise the whole or any part of this COP and publish further guidelines and other requirements for operation of the eHRSS.

2. CODE OF PRACTICE FOR MANAGEMENT EXECUTIVES, ADMINISTRATTIVE AND TECHNCIAL STAFF

2.1. REGISTRATION OF HEALTHCARE PROVIDERS IN EHRSS

2.1.1. Healthcare providers meeting the registration requirements set out in eHRSSO may apply to the eHRC for registration in eHRSS.

2.1.2. eHR healthcare providers should maintain an updated registration record , including business registration, contact persons, details of participating hospital(s) or clinic(s) and service locations…etc. They should inform eHRC timely for changes in business nature and clinical services and provide all necessary supporting information for verification. (Please refer to the *Guidelines and Procedures for Registration of HCP* for a complete checklist of the information /documents that must be submitted and the administrative procedures for registration).

2.1.3. eHR healthcare providers should withdraw from eHRSS if they no longer fulfil the registration requirements e.g. change of nature of services or termination of business.

2.1.4. eHR healthcare providers should understand and fulfil the conditions of registration for Electronic Health Record Healthcare Provider set by the eHRC.

2.1.5. eHR healthcare providers should be aware that their registration may be suspended or cancelled by eHRC due to breaching of any specified requirement set out by eHRC. Any such suspension or cancellation in registration may affect sharing of their HCRs' records in eHRSS.

2.2. HANDLING REGISTRATION OF HCR

2.2.1. eHR healthcare providers should observe the operational and administrative requirements set out by the eHR Office for registering HCRs in eHRSS. (Please refer to the *Guidelines and Procedures for HCR Registration* for registration of capable adults, minors, new-born, mentally incapacitated persons and persons incapable of giving consent and registration matters when eHRSS is notified that a HCR has died)

2.2.2. eHR healthcare providers should verify the identity of the HCR and check if the HCR holds:

(a) an HK Identity Card;

(b) a certificate of registration of birth issued underthe Births and Deaths Registration Ordinance (Cap. 174);

(c) a proof of identity as defined by section 17B(1) (other than an identity card) of the Immigration Ordinance (Cap. 115);

(d) a certificate of exemption as defined by section 17G(1) of the Immigration Ordinance (Cap. 115); or

(e) any other identification document specified by the Commissioner.

2.2.3. eHR healthcare providers should ensure accurate capture and verification of HCR's information during registration.

2.2.4. eHR healthcare providers should submit a copy to the eHR Office and retain appropriate original supporting documents for verification.

2.2.5. eHR healthcare providers should understand the conditions which would allow Substitute Decision Maker (SDM) to act for HCRs incapable of giving consent in registration and related procedures.

2.2.6. eHR healthcare providers should ensure their administrative staff handle HCRs' and/or SDM's HKIC with care and in accordance with the *Guidelines and Procedures for Using Hong Kong Identity Card (HKIC) for eHRSS* and *Guidance for Using Personal Identifier* issued by the PCPD for handling HCRs registration and consent matters.

2.2.7. eHR healthcare providers should ensure HCRs and their SDMs understand and agree with the conditions and purpose of using their personal data for registration and giving consent in relation to:

(a) Giving consent to join eHRSS;

(b) Giving sharing consent to healthcare providers; and

(c) Updating registration information (e.g. HCR withdrawing from eHRSS or revoking consent to a healthcare provider).

2.2.8. eHR healthcare providers should update demographic information of their HCRs and their SDMs and timely inform eHR Office of any amendments and update in major identification keys (e.g. HCR's Names, Sex, Date of Birth, Hong Kong Identity Card number or Other Travel Document Numbers).

2.3. OBTAIN HCR's CONSENT FOR EHR ACCESS

2.3.1. eHR healthcare providers should obtain express, informed consent from HCRs or their SDMs (if applicable) for:

(a) registration in eHRSS and

(b) sharing of their health information through the eHRSS

2.3.2. eHR healthcare providers should take the following actions to ensure HCR's or his/her SDM's consent (if applicable) is valid and well-informed by:

(a) Providing sufficient, relevant and comprehensible information (e.g.

Patient Information Notice, pamphlets, posters…etc.)

(b) Obtaining consent from SDM for HCRs who are incapable of giving consent; and

(c) Requesting the HCR or their SDM to confirm that their consent is voluntary

2.3.3. eHR healthcare providers should be aware of the general principles of handling consent by HCRs:

(a) A person can give consent to register for or withdraw from eHR sharing, and to give or revoke sharing consent unless he/she is a minor under age 16 or there is evidence that he/she is incapable of giving consent.

(b) For minors and HCR who are incapable of giving consent, consent should be given by their SDMs.

2.3.4. eHR healthcare providers should be acquainted with the types of persons eligible to act as a SDM for a particular class of HCR as stipulated by the eHRSSO, who may give a substitute consent for that class of HCR to register or withdraw from eHRSS and to give sharing consent to HCP(s). eHR healthcare providers should always respect the HCR's own expressed preference. If the HCR could clearly express his/her intent, the Healthcare Providers should carefully assess whether his/her case indeed require any SDM.

2.3.5. eHR healthcare providers should be aware that where there is no other eligible SDM available and the healthcare providers consider that it is in the best interest for the HCRs, the healthcare providers can choose to give consent for registration and sharing in the eHRSS under the Ordinance (eHR healthcare providers should appoint designated person under its charges to perform the tasks of the SDM of the HCRs).

2.3.6. eHR healthcare providers should be aware that there are two types of Sharing Consent: "Indefinite Sharing Consent" & "One-year Sharing Consent".

2.3.7. eHR healthcare providers should be aware that "Indefinite Sharing Consent' is in effect until it is revoked or the registration of the HCR is withdrawn or cancelled.

2.3.8. eHR healthcare providers should be aware that "One-Year Sharing Consent" to healthcare providers is valid for one year unless it is revoked or the registration of the HCR is withdrawn or cancelled.

2.3.9. eHR healthcare providers should not share health information of HCRs through eHRSS who have withdrawn from registration or revoked their sharing consent.

2.3.10. eHR healthcare providers should be aware that HCRs will receive a notification from eHRSS for access to their eHR in the form chosen by the HCRs including but not limited to the following:

(a) Electronic message (e.g. Short Message Service (SMS));

(b) Postal mail; and

(c) e-mail

2.3.11. eHR healthcare providers should provide HCRs with access to their organizations' privacy policy document(s) and information about the kinds of data that will be shared and the purposes of sharing to eHRSS.

2.4. EHR HEALTHCARE PROVIDERS TO MANAGE HCS' USER ACCOUNT

2.4.1. eHR healthcare providers should be responsible for registering and maintaining their HCS' user accounts including checking and updating professionals registration status if appropriate for all healthcare professionals working in the eHRSS for validation in a timely manner according to the *Guidelines and Procedures for HCS Registration*. eHR healthcare providers should close the accounts of departing staff before their last day of service.

2.4.2. eHR healthcare providers should issue appropriate authentication means (e.g. security token), according to the guidelines issued by the eHR Office to their healthcare professionals to access eHRSS.

2.4.3. eHR healthcare providers should ensure only authorized healthcare professionals with the need to know about the health information of the HCRs for the purpose of providing healthcare can access to eHR of HCRs.

2.4.4. eHR healthcare providers should ensure their staff respect and have adequate awareness and knowledge of personal privacy, information confidentiality and system security.

2.4.5. eHR healthcare providers should ensure that their HCS are aware that using HCRs' information from eHRSS for direct marketing is forbidden.

2.4.6. eHR healthcare providers should take reasonable and practicable steps to ensure their healthcare professionals properly use security controls and devices (e.g. log-in password and security tokens).

2.4.7. eHR healthcare providers should appoint administrative and technical staff, as contact person(s) to communicate with the eHR Office.

2.4.8. eHR healthcare providers should supervise and monitor staff carrying out administrative and technical duties, including but not limited to:

(a) Registering and managing information of healthcare providers in eHRSS;

(b) Registering and managing information of HCRs in eHRSS;

(c) Registering and managing information of healthcare professionals in eHRSS;

(d) Performing regular reporting, exceptional reporting and cooperating with eHR Office in audit on eHR operations

2.5. MANAGE HEALTHCARE PROVIDERS' OWN CLINICAL RECORDS

2.5.1. eHR healthcare providers should maintain clear and updated clinical records for their HCRs. eHR should not be taken as a replacement of a healthcare providers' own HCR records.

2.5.2. eHR healthcare providers should ensure the data in their medical record system is accurate for sharing.

2.5.3. eHR healthcare providers should share the health information of their HCRs who have consented to the sharing of their health records in eHRSS if the information is readily available and sharable after each episode of care as soon as possible .

2.6. MAKE DATA SHARING SECURED

2.6.1. eHR healthcare providers will be notified by eHR Office of the standards, policies and requirements on security and interfacing for data sharing between their eMRs or ePRs with eHRSS. eHR healthcare providers should endeavour to comply with these requests. (List of detailed requirement documents will be distributed and available for registered eHR HCPs and their relevant staff)

2.6.2. eHR healthcare providers should perform self-assessment and tests with eHR Office for data readiness and interoperability before sharing information to eHRSS according to the *eHRSS Data Interoperability Standards*.

2.6.3. eHR healthcare providers should perform system connection testing with the eHR Office for data sharing according to security requirements and other specifications according to the *eHRSS Data Requirement Specification document*.

2.6.4. eHR healthcare providers should provide amended and updated records in their eMR to eHRSS if previous records have been shared to eHRSS.

2.6.5. eHR healthcare providers should maintain relevant system audit logs about access to eHRSS through their eMR systems *according to the eHR IT Security Policy.*

2.6.6. eHR healthcare providers should perform regular monitoring and audit on system behaviour for identification of abnormality, intrusion and potential system fault or user misbehavior.

2.6.7. eHR healthcare providers should report as soon as possible to eHR Office any suspected security incidents, privacy incidents and suspected security weakness related to using eHRSS.

2.6.8. eHR healthcare providers should perform periodic Security Risk Assessment and Audit (SRAA) of their own eMR systems or perform security assessment and fix any identified security loop holes according to the requirements specified by the eHR Office for system connection according to the *eHR Connection Mode Guide*. Any identified security risks or non-conformance with the security requirements should be rectified in a timely manner.

2.6.9. eHR healthcare providers should cooperate with eHR Office for auditing or investigations if necessary.

2.6.10. eHR healthcare providers should provide adequate security and privacy awareness training for their healthcare staff proper using of eHRSS.

2.6.11. eHR healthcare providers should implement, and maintain the implementation of, the security measures relating to the eHRSS which are prescribed from time to time by the eHR Office:

(a) Keep and access only enabled computers (i.e. with appropriate certification software) in secured physical locations (e.g. access within secured workplace, clinic or office) and avoid access to eHRSS in public areas such as internet cafe or public library;

(b) Keep and maintain security in wired and wireless network for computers connecting to eHRSS

(c) Keep computer system and software updated with latest security patches applied;

(d) Use only licensed / legal computer software and with latest security patches applied and avoid using peer-to-peer software (e.g. Foxy or Bit Torrent…etc.);

(e) Install appropriate anti-virus and anti-spyware software;

(f) Ensure staff logoff eHRSS and local EMR systems after use;

(g) Enable automatic screen-lock or screen-saver with password protection on computer workstation and set up of a reasonable idle time;

(h) Ensure staff should observe password policies (e.g. use of strong sword with regular updates, avoid writing down or sharing of password; change the eHRSS system assigned password immediately after successful login for the first time);

(i) Record and manage access rights assigned to each authorized staff according to their roles in delivering healthcare to the patients and;

(j) Assign individual account for each user and ensure them use properly any means of security log-on measures or devices (e.g. log-in password and security token) and protect them against unauthorised use (e.g. sharing with others)

2.7. HANDLING DATA ACCESS REQUEST AND DATA CORRECTION REQUEST

2.7.1. eHR healthcare providers should advise HCRs to approach eHR Office for Data Access Request for eHR data contained in eHRSS.

2.7.2. eHR healthcare providers should handle Data Correction Request in accordance with the relevant provisions in PD(P)O and eHRSSO.

2.7.3. eHR healthcare providers should be aware that Data Correction Request for *demographic* data (e.g. Name, Identity Number, Date of Birth or Sex) in eHRSS can be handled by both eHR Office or a prescribed eHR HCP

2.7.4. eHR healthcare providers should be aware that Data Correction Request for the HCRs' *clinical data* in the eHRSS should be reviewed by the healthcare providers who have contributed and shared that information to eHRSS according to established workflow for handling of such requests by the eHR Office. (*Policy and Guidelines for Handling DAR & DCR in eHRSS*)

2.7.5. eHR healthcare providers should update and provide corrected clinical records to the eHRSS as soon as possible once an error of their HCR's record is noted and rectified.

2.7.6. eHR healthcare providers should exercise careful judgement to handle the data correction request and to inform the HCRs and eHR Office the result of such requests and the reason of refusal if the request is refused.

2.7.7. eHR healthcare providers should make a note and attach a note to the HCR's record and provide to eHRSS if the Data Correction Request is refused and the data to which it relates is an expression of opinion according to the PD(P)O.

3. CODE OF PRACTICE FOR HEALTHCARE PROFESSIONALS

3.1. MAINTAINING USER ACCOUNT

3.1.1. eHR healthcare professionals will be provided a user account in eHRSS through the healthcare provider(s) they work with.

3.1.2. eHR Healthcare professionals should provide the eHRSS with updated professional registration information.

3.2. UPDATE RECORDS FOR EHR SHARING

3.2.1. eHR healthcare professionals should keep clear, accurate and updated clinical records of their HCR and share to eHRSS in a timely manner.

3.2.2. eHR healthcare professionals should comply with PD(P)O in collecting information in their HCRs' records and make sure it is accurate and not excessive.

3.2.3. eHR healthcare professionals should advise HCRs to approach the original HCP who provide the specific information to eHRSS for data correction if they notice any genuinely incorrect information in their eHR which is provided by other HCPs or healthcare professionals. It is advisable to document such observation in their HCRs' records.

3.2.4. eHR healthcare professionals should have duty and responsibility to assist their respective healthcare providers to deal with any data correction request for any alleged incorrect information in their HCRs' clinical records that has been shared to eHRSS in a manner and within a time frame as specified under PD(P)O.

3.2.5. eHR healthcare professionals should exercise careful judgment for accepting or refusing a data correction request from their HCRs. If they are not satisfied that the information to which the request relates is inaccurate and they should inform HCRs or the data requesters the decision and reasons of refusal.

3.2.6. eHR healthcare professionals should document the reasons for refusal for data correction request in their HCR's records and inform eHR Office if the data in dispute is an expression of opinion in accordance with the PD(P)O

3.3. POINTS TO NOTE WHEN ACCESSING A HCR’S EHR

3.3.1. eHR healthcare professionals should ensure their access to a HCR’s eHR is under authorisation and with the need to know for the purpose of providing healthcare to the HCR.

3.3.2. eHR healthcare professionals should have the responsibility to exercise judgement on clinical grounds on whether and how much information from a HCR’s eHR should be accessed for reference purposes.

3.3.3. eHR healthcare professionals should have the autonomy and professional judgment to interpret the information on eHRSS.

3.3.4. eHR healthcare professionals should access only to the HCRs’ eHR, from whom a valid consent has been obtained. As a matter of good practice, it is advisable for healthcare professionals to inform their HCRs their eHR is to be accessed. In any event, after each access the HCRs will be notified by the system of the access.

3.3.5. eHR healthcare professionals are advised to inform their HCRs that access to their eHR beyond usual consultation time is possible for valid reasons (e.g. before-clinic visit preparation or after-clinic follow-up care).

3.3.6. eHR healthcare professionals should be aware that each access will be subject to audit and HCRs or their SDM will be notified about access to their eHRs.

3.3.7. eHR healthcare professionals should be aware that, for any HCR who is incapable of giving sharing consent to healthcare providers for eHR access, the healthcare professionals may gain emergency access to the eHR of the HCR if that is of paramount importance for provisions of emergency treatment to the HCR. eHR healthcare professionals are advised to document such access in their HCRs’ record and the justification in the eHRSS and should be aware that such emergency access is subject to audit.

3.4. POINTS TO NOTE WHEN VIEWING AND USING EHR

3.4.1. eHR healthcare professionals should interpret information from eHRSS with care as it may not be updated and complete. They should judge there is a need to verify with other sources of information, and ideally, with the HCR, especially when in doubt or inconsistency is noted.

3.4.2. eHR healthcare professionals should not regard eHR as a substitute for personal communication with their HCRs and other healthcare professionals.

3.4.3. eHR healthcare professionals should record and document relevant important decisions and discussions with their HCRs based on the information from eHRSS (including date / time of information being created and accessed, significant findings and conclusion after discussion with HCRs. . .etc.).

3.4.4. eHR healthcare professionals should be aware that they have no obligation to copy all information from the eHRSS into their own HCRs' records.

3.4.5. eHR healthcare professionals should clearly indicate the source of information, date / time of the information being accessed when copying information from eHRSS in their own HCRs' records.

3.4.6. eHR healthcare professionals should not use information from eHRSS for writing reports for third parties (e.g. insurance claims or health check report). Reports for third parties should be based on the healthcare professionals' own clinical records and/or assessment of the HCRs.

3.4.7. eHR healthcare professionals should exercise diligence of care in explaining any information accessed through eHRSS to HCRs and not to use them for alleging challenges or criticism in whatever means to depreciate the professional skills, knowledge services or qualification of other healthcare professionals and/or healthcare providers.

3.5. RESPECT CONFIDENTIALITY OF HCR'S INFORMATION

3.5.1. eHR healthcare professionals should respect confidentiality of information obtained from eHRSS.

3.5.2. eHR healthcare professionals should be aware that each access to HCR's eHR will be logged and monitored.

3.5.3. eHR healthcare professionals should ensure prior and express consent is obtained from the HCRs before disclosure any information obtained from eHRSS to any third party.

3.6. ENQUIRIES AND ASSISTANCE

3.6.1. Staff designated by Healthcare Providers as contact points may approach eHR Office for assistance via e-mail (xxx) or telephone (xxx).

4. ANNEX

4.1. SDM ARRANAGEMENT FOR EHR SHARING

Persons who have given express and informed consent to join eHRSS would be registered in the eHRSS. HCRs registered must give further separate consent to individual healthcare providers(s), from whom they receive healthcare from, to enable those particular healthcare providers to share their records in the eHRSS. Sharing consent to a healthcare provider could be either an “indefinite” or “one-year” consent.

To enable certain HCRs who are incapable of making an informed decision to share their health data, the eHRSSO stipulates that the following types of person can act as “substitute decision makers” (SDMs) to give consent on behalf of these HCRs:

Persons incapable of consenting	Persons who may act as SDM
(a) A minor (below 16)	1. Parents 2. Guardian 3. Persons appointed by court 4. Immediate Family Members 5. HCP
(b) HCR who is not a minor but being incapable for giving consent	1. Guardian 2. Director of Social Welfare 3. Persons appointed by court 4. Immediate Family Members 5. HCP

4.2. HEALTHCARE PROVIDERS IN EHRSS

Healthcare Provider is a person that provides healthcare at one service location may apply to the Commissioner to be registered as a healthcare provider for the System for the location.

A person provides healthcare at one service location if the person –

a. is registered under section 3(4) of the Hospitals, Nursing Homes and Maternity Homes Registration Ordinance (Cap 165) in respect of one hospital or one maternity home;

b. is registered under section 5(2) of the Medical Clinics Ordinance (Cap 343) in respect of one clinic;

c. carries on the business of dentistry under section 12 of the Dentists Registration Ordinance (Cap 156) at one place;

d. holds a certificate of exemption issued under section 7(2), or a licence issued under section 8(2)(a), of the Residential Care Homes (Elderly Persons) Ordinance (Cap 459) in respect of one residential home and engages a healthcare professional

e. holds a licence issued under section 7(2)(a), or a certificate of exemption issued under section 11(2)(a), of the Residential Care Homes (Persons with Disabilities) Ordinance (Cap 613) in respect of one residential home for PWDs and engages a healthcare professional

f. is a specified entity that engages a healthcare professional to perform healthcare at one place; or

The Commissioner may register a Government bureau or department as a healthcare provider for the System if the Commissioner is satisfied that the operation of the bureau or department involves the provision of healthcare.

4.3. HEALTHCARE PROFESSIONALSREGISTERED IN EHRSS

The following healthcare professionals are allowed for sharing in eHRSS:

1. Registered medical practitioner (Cap 161);
2. Registered nurse or enrolled nurse (Cap 164);
3. Registered midwife (Cap 162);
4. Registered dentist (Cap 156);
5. Registered pharmacist (Cap 138);
6. Registered medical laboratory technologist (Cap 359A);
7. Registered radiographer (Cap 359H);
8. Registered dental hygienist (Cap 156B);
9. Registered chiropractor (Cap 428);
10. Registered occupational therapist (Cap 359B);
11. Registered optometrist (Cap 359F);
12. Registered physiotherapist (Cap 359J); and
13. Registered and listed Chinese medical practitioner (Cap 549).

Sharing by different healthcare professionals at different phrases will be reviewed from time to time and announced by eHR Office.

4.4. POLICIES, GUIDELINES & PROCEDURES AND OTHER RELEVANT INFORMATION RELEASED BY EHR OFFICE FOR PARTICIPATING IN EHRSS

General Policies and Guidelines

(a) Patient Information Notice

(b) Conditions for eHR HCP Registration

(c) Guideline for Using eHR Data for Research and Statistics

(d) eHRSS Privacy Policy Statement

(e) eHRSS Personal Information Collection Statement

(f) Guidelines and Procedures for eHR Healthcare Recipient Registration

(g) Guidelines and Procedures for eHR Healthcare Provider Registration

(h) Guidelines and Procedures for eHR Healthcare Staff Registration

(i) Management of Healthcare Recipient Index

(j) eHR Data Retention Policy

(k) Policy and Guidelines for Handling DAR & DCR in eHRSS

(l) Guidelines and procedures for using Hong Kong Identity Card for eHR

(m) FAQs on eHR Data for Research and Statistics

(n) FAQs on eHRSS

eHR Data Standards

(o) eHR Content Standards Guidebook.

(p) Editorial Guide on Hong Kong Clinical Terminology Table – Overview.

(q) Guide on Implementation & Maintenance of the Hong Kong Clinical Terminology Table.

(r) eHRSS Data Requirement Specification

eHR Security and System Connection Guidelines

(s) IT Security Policies for eHRSS

(t) Security Assessment Checklist for Participating in the eHR Programme

(u) eHR Connection Mode Guide

(v) eHRSS Data Interoperability Standards

(w) Communication Protocol (Data Interface) Specification

(x) ELSA Installation Guide

(y) Token Inventory Management User Guide

(z) eHR Adaptor Interface Specification

(aa) Process Report and Exceptional Reporting Requirement

4.5. REFERENCE FROM THE OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA (PCPD)

Office of the Privacy Commissioner for Personal Data
(http://www.pcpd.org.hk/)
Personal Data (Privacy) Ordinance (Cap 486)
(http://www.pcpd.org.hk/english/ordinance/ordfull.html)
Data Protection Principles
(http://www.pcpd.org.hk/english/ordinance/ordglance.html)
Code of Practice
(http://www.pcpd.org.hk/english/ordinance/codes.html)
Guideline and Explanatory Booklet
(http://www.pcpd.org.hk/english/publications/code_pra_ex.html)
Guidance Note & Fact Sheet
(http://www.pcpd.org.hk/english/publications/guid_note.html)
Information Book
(http://www.pcpd.org.hk/english/publications/infor_book.html)
Guidance on Data Breach Handling and the Giving of Breach Notifications
(http://www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf)

The references listed out in this COP are by no means exhaustive. The Office of the Privacy Commissioner for Personal Data may issue more Code of Practice or Guideline Note or other material or update any existing documents from time to time. Readers of this COP are advised to access to the internet website of the Office of the Privacy Commissioner for Personal Data for the most updated information (http://www.pcpd.org.hk/).

附件 C

電子健康紀錄互通系統處理投訴機制草擬框架

(注意：此文件屬初步草稿，只是大致顯示將來最終處理有關電子健康紀錄互通系統(互通系統)運作的投訴的機制)

整體原則(*需涵蓋的事項*)

- 公平 (例如，根據投訴內容的重要性、所收投訴的日期、延誤所引致的不利後果等給予優先次序;被投訴的當事人不可親自處理投訴)
- 一致 (例如，向處理投訴的人員給予足夠的指引和培訓，以一致的做法和程序處理投訴)
- 公開及透明 (例如，讓投訴人知悉有關的進度和結果)
- 便利 (例如，有效和有足夠宣傳的投訴渠道；回覆投訴人的書面溝通應以簡易的語文，和盡量使用與投訴人相同的語言)
- 保密 (例如，一般而言，有關所收投訴的資料和投訴人的個人資料應以有需要知道原則發布；為遵守《個人資料(私隱)條例》(私隱條例，第 486 章)，如有需要將個人資料給予第三方，須事先獲得投訴人(資料當事人)的同意)

提出投訴渠道，例如

- 親身提出
- 電話
- 郵寄
- 電郵
- 傳真

投訴人需要提供的資料

- 投訴人的個人資料
- 投訴人的聯絡方法
- 被投訴者的身份
- 個案詳情
- 證明文件，如有

初步處理及篩選

- 發出書面認收函件
- 編配個案編號及負責處理投訴人員
- 記錄投訴人提供的資料及有需要時向投訴人索取進一步的資料

- 檢視投訴人提供的資料，及向有關人士/機構(包括被投訴者)收集資料/意見後決定表面證據是否成立(不透露投訴人的身份/個人資料)
- 將不合乎電子健康紀錄專員職權範圍的個案轉介相關機構跟進，例如
  - 有關使用電子健康紀錄的個人資料時涉嫌違反私隱條例的投訴：轉介個人資料私隱專員公署
  - 有關貪污及賄賂等的投訴：轉介廉政公署
  - 有關涉嫌觸犯在電子健康紀錄條例下的刑事罪行的投訴：轉介相關執法部門(如警務署)
- 如個案需要被轉介，須在轉介前向投訴人徵求同意
- 如個案表面證據不成立，通知投訴人原因及他/她的其他選擇(例如要求覆檢，提出上訴)

<u>進一步處理(表面證據成立而不需要轉介的個案)</u>

- 根據與投訴性質相關的政策及指引研究個案，和負責的相關組別收集有關投訴的資料，例如
  - 投訴有關互通系統的技術性事宜(如系統故障,互通資料不準確)：資訊科技小組；互通系統數據互用標準，互通系統數據需求規格等
  - 投訴有關職員的態度及表現：相關已制定的公務員指引，例如有關行為和紀律
  - 投訴有關拒絕/暫時吊銷/取消醫護提供者/(登記)醫護接受者的登記：登記小組
- 如有需要，向投訴人索取進一步資料
- 向被投訴者採取適當的進一步行動
  - 要求採取補救措施
  - 口頭警告
  - 書面警告
  - 暫時吊銷在互通系統的登記(只適用於投訴醫護提供者/醫護接受者的個案)
  - 取消在互通系統的登記(只適用於投訴醫護提供者/醫護接受者的個案)
- 通知投訴人投訴結果及可行的選擇，例如要求覆檢/提出上訴(就口頭投訴，口頭回覆一般而言已經足夠。如投訴人要求書面回覆，則提供書面回覆)

覆檢/上訴

- 投訴人可透過負責人員，就其投訴的處理方法要求覆檢，或就結果提出上訴。如情況可行，處理這些要求的人員，職級應高於原先的負責人員。
- 任何人如因電子健康紀錄專員拒絕 / 暫時吊銷 / 取消醫護提供者 / (登記)醫護接受者的登記的決定而感到受屈，可向行政上訴委員會提出上訴。

職員的角色

- 處理投訴的負責人員：不低於高級行政主任或同級的人員
- 對醫護提供者/醫護接受者作出重大處分(例如暫時吊銷/取消登記)的最終決定：電子健康紀錄專員

整體處理時間

- 由於互通系統至今仍未運作，因此我們沒有運作上的經驗可參考，我們預計：
  - ■ 就一般個案，應在十個曆日內覆函認收，並在接獲投訴後 30 個曆日內發出具體答覆
  - ■ 就需要較長時間處理的複雜個案，應通知投訴人個案的進度及需要較長時間作出具體答覆的原因

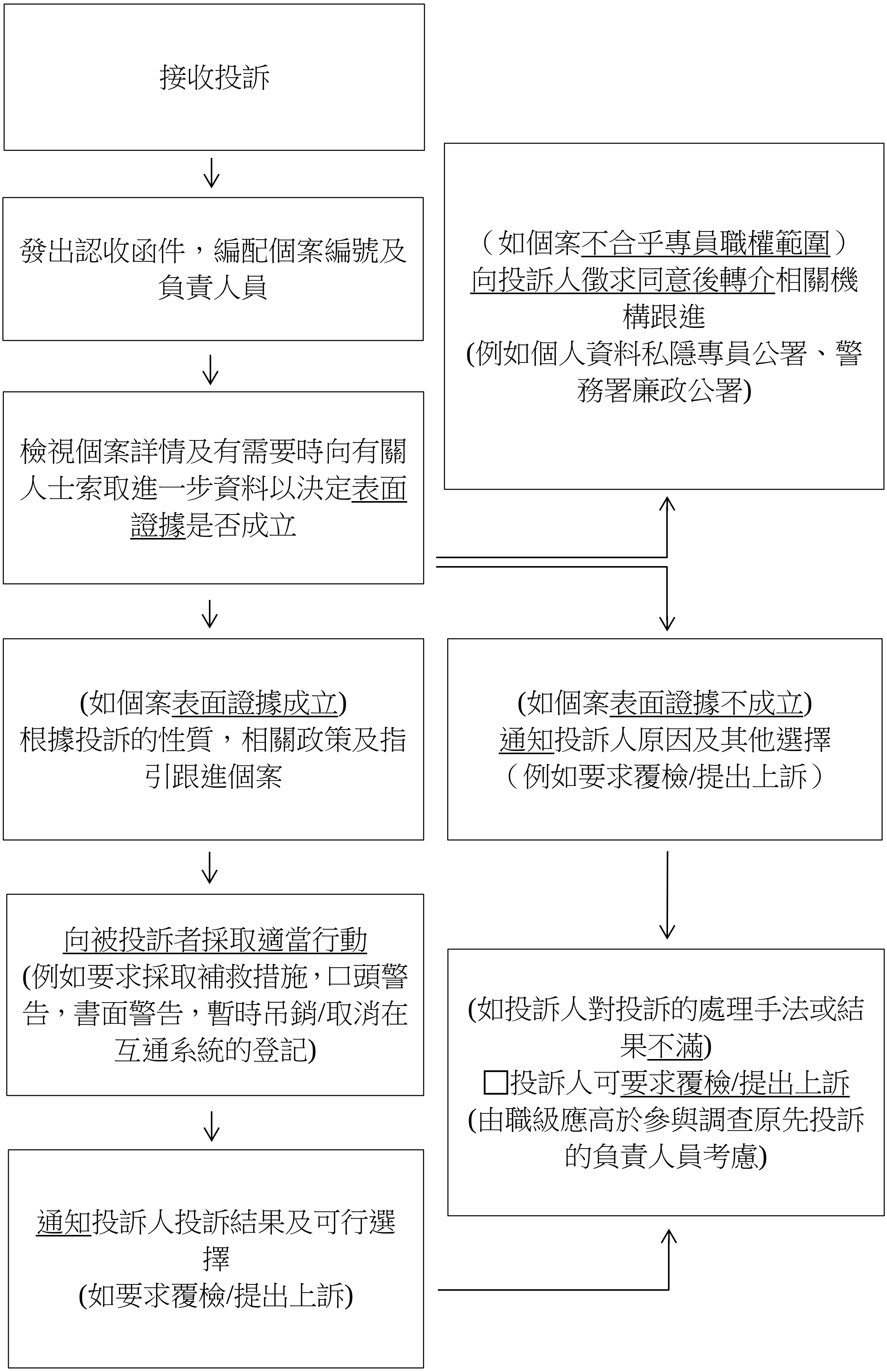
進度監察

- 所有書面或口頭提出的投訴，均應記錄於中央投訴登記冊。登記冊內應包含每宗投訴的足夠資料以監察進度，及將來在需要的情況下作出檢討。
- 負責人員有責任更新有關進度，亦須注意長期未完成的個案和留意投訴的跟進行動。

匿名投訴

- 視乎指控的嚴重性及是否有足夠資料作有有意義的調查，若干匿名投訴也應視作其名投訴般處理，儘管無法給予投訴人回覆。

主要步驟的說明性流程表



接收投訴

發出認收函件，編配個案編號及負責人員

檢視個案詳情及有需要時向有關人士索取進一步資料以決定表面證據是否成立

（如個案不合乎專員職權範圍）
向投訴人徵求同意後轉介相關機構跟進
(例如個人資料私隱專員公署、警務署廉政公署)

(如個案表面證據成立)
根據投訴的性質，相關政策及指引跟進個案

(如個案表面證據不成立)
通知投訴人原因及其他選擇
（例如要求覆檢/提出上訴）

向被投訴者採取適當行動
(例如要求採取補救措施，口頭警告，書面警告，暫時吊銷/取消在互通系統的登記)

(如投訴人對投訴的處理手法或結果不滿)
□投訴人可要求覆檢/提出上訴
(由職級應高於參與調查原先投訴的負責人員考慮)

通知投訴人投訴結果及可行選擇
(如要求覆檢/提出上訴)