Building a Healthy Tomorrow

Discussion Paper on The Future Service Delivery Model for our Health Care System

Authored by

The Health and Medical Development Advisory Committee ~ Health, Welfare and Food Bureau

Submission by The Office of the Privacy Commissioner for Personal Data

October 2005

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Table of Contents

1 Preamble

The Office of the Privacy Commissioner for Personal Data ("the PCO") is an independent statutory authority which began operation in December 1996. The Commissioner for Personal Data Privacy ("the Commissioner") and his staff are charged with the following responsibilities.

- Administering the Personal Data (Privacy) Ordinance ("the Ordinance");
- Monitoring and supervising data users compliance with the provisions of the Ordinance to ensure that they honour the responsibilities that those provisions place upon them;
- The inspection of personal data systems including those of HKSAR Government departments and statutory organizations;
- Protecting the personal data privacy rights conferred upon data subjects by the Ordinance and the prospect of guarding against any encroachment upon, dilution of or technological challenges to those rights.

2 The PCO welcomes the opportunity to comment upon proposals presented in the Discussion Paper prepared by the Health and Medical Development Advisory Committee ("the Discussion Paper") and, in particular, the personal data privacy issues that may arise from paragraphs 9.4 and 9.5 under the heading of ***Promotion of free flow of patient records.*** Specifically, the substance of this submission is confined to the personal data privacy issues associated with the following statements contained in the Discussion Paper:

Paragraph 9.4

"... it is essential to develop a system which enables free flow of patients' records with the patient's consent."

Paragraph 9.5

"The short-term aim should be to provide patients of all General Out-patient Clinics and SOPDs with hand-held record and to encourage private doctors to do the same. In the long term, we believe that there should be the development of a territory-wide

information system for carers in both the public and private sectors to enter, store and retrieve patients' medical record."

In seeking to place the contents of this submission in context the PCO takes the view that the above suggestions imply the establishment of an *electronic* database that would contain patients' medical records whether they be comprehensive or partial records of the individual. The PCO assumes that any patient medical records database established to facilitate the delivery of health care in Hong Kong would be accessed by a diverse range of professional health care providers, subject to protocols being in situ that would restrict authorized access to the database.

2 Background to Personal Data Privacy in the HKSAR

Personal data privacy[1] in the HKSAR, as distinct from privacy in its more generic sense, is legally protected under the provisions of the Ordinance. The Ordinance gives legal force to six Data Protection Principles ("DPP" - please refer to Appendix I). These six principles have legal ramifications for the Health, Welfare and Food Bureau if it were to establish an electronic database containing patients' medical records. The data contained in such records are invariably regarded as being the most sensitive category of personal data and for this reason the measures taken to prevent accidental and unauthorised access and use of the database need to be meticulously documented, effectively managed and constantly policed.

2.2 The DPP form the cornerstone of the Hong Kong Ordinance and similar data protection principles underline comparable legislation in other countries. Many countries draw heavily upon the pioneering work of the OECD guidelines.[2] Those guidelines were first promulgated in

---

The Personal Data (Privacy) Ordinance defines "personal data as any data –

a) relating directly or indirectly to a living individual;
b) from which it is practicable for the identity of the Individual to be directly or indirectly ascertained; and
c) in a form in which access to or processing of the data is practicable.

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). The Guidelines can be viewed in full at:
http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html.

1980 to provide a framework for the protection, collection and use of personal data.

The DPP contained in the Ordinance may be summarized as follows.

- **Principle 1 - The Purpose and Manner of Collection**
  Principle 1 provides for the lawful, fair and non-excessive collection of personal data. It also establishes the information a data user must provide to the data subject prior to, or at the time of the collection of personal data, from the data subject. In the context of the Discussion Paper the data subject is the patient. The purpose of the collection of personal data should be notified to data subjects in writing in the form of a Personal Information Collection Statements ("PICS").

- **Principle 2 - The Accuracy and Duration of Retention**
  Principle 2 provides that personal data should be accurate, up-to-date and kept no longer than necessary for the fulfillment of the purpose for which the data are to be used.

- **Principle 3 - The Use of Personal Data**
  Principle 3 provides that unless the data subject gives prior consent, personal data should only be used for the purpose(s) for which it were collected, or a directly related purpose.

- **Principle 4 - The Security of Personal Data**
  Principle 4 requires the data user to take all practicable steps to ensure that appropriate security measures are in place to protect against unauthorized or accidental access, processing or erasure of personal data.

- **Principle 5 - Information to be Generally Available**
  Principle 5 provides for transparency on the part of data users regarding the types of personal data they hold and the main purposes for which personal data are used. This is interpreted to mean that data users should formulate, and make available, a privacy policy statement ("PPS").

- **Principle 6 - Access to Personal Data**
  Principle 6 provides for individuals to have the right of access to, and correction of, their personal data held by a data user.

2.3 It can be seen from this summary of the six DPP that the Ordinance not only protects the personal data privacy of individuals, but also confers rights upon them. It is the Commissioner's considered opinion that the impact of these principles upon the proposals contained under paragraphs 9.4 and 9.5 of the Discussion Paper warrants a serious and detailed study *before* a final decision is taken on the establishment of a patient medical records database to ensure that there be full compliance with the provisions of the Ordinance.

3 Privacy Concerns Commonly Associated with Medical Record Databases

3.1 The highly sensitive nature of patient medical data, integration of records and their concentration in a database, creates the concern that any breach of the integrity of the database could be seriously harmful to the interests of patients. There can be little doubt that it is very difficult to guarantee the security of any database that may be accessed by a large number of file users. Even where access is subject to strict protocols, systems managed by institutions such as the HSBC, Microsoft and the FBI have been unlawfully accessed by unscrupulous IT experts using sophisticated means. That being so, there is a good case for the development of a patient medical records database to be preceded by scenario planning with a view to anticipating the range of possible outcomes, and response to them, in the event of the accidental or unlawful access and use of patient medical data.

3.2 In reviewing the possible vulnerabilities of a patient medical records database some observers have noted that the patient may actually benefit from a manual medical record system in that they would need to be physically stolen as distinct from being electronically downloaded from a database. Secondly, it is likely that a manual system would tend towards being more piecemeal, and therefore a less than comprehensive record, because patients may have benefited from health care provided by multiple doctors, clinics and out patient departments. In contrast, a database system would both integrate and concentrate medical records giving a more comprehensive picture of the medical history of the individual. Inevitably therefore the existence of a patient medical records database may pose issues that are less of a problem in manual

record systems. This argument has, notably in the USA, given rise to the growth and influence of privacy lobby groups that seek to draw attention to the vulnerabilities of medical record databases. A system with an 'open' architecture, that permits the accessing and/or downloading of patient records, suggests the desirability for a balance to be struck between the medical benefits to be derived from such a system and the potential risk posed to the privacy of those whose medical history is entered in the system.

3.3 Authorisation to access computerized medical records gives rise to at least two issues. The first of these relates to public perceptions of trust and confidence. Will the system effectively manage the potential problems of accidental and unauthorized access to, and use of, medical records contained in it? Secondly, database security protocols notwithstanding, what guarantees can be offered to the public in terms of data security? That is, the interception of patient medical data in transmission to an authorized users terminal or when stored in a backend system?

3.4 Such concerns are not academic. The Health Privacy Project Medical Privacy Stories - Appendix II - contains a selection of real-life incidents that occurred in the USA alone. These reports[3] indicate malpractices and high-light the concerns that will need to be addressed by the Health, Welfare and Food Bureau if they are to win the confidence of patients and their consent to having their medical records placed in the system proposed. Clearly if those conditions are not met then there is the prospect of a large number of patients electing to opt-out of the system which could well undermine its utility.

3.5 In March 2005, the Institute for Health Freedom in the USA reported on a Harris Interactive Poll,[4] conducted in February of this year, which investigated Americans' attitudes towards government plans for a

[3] The Medical Privacy Stories cited by the Health Privacy Project relate to accidental or unauthorised access, poor security and disposal of records, medical information used for marketing, government use of records, researchers, law enforcement and lawsuits. Further details of the stories can be found in Appendix II.

The telephone survey was conducted in a nationwide survey o 1,012 adults aged 18 and over.

national Electronic Medical Records ("EMR") System.[5] A summary of the findings of the survey indicate a level of ignorance on the part of respondents and significant concerns regarding EMR.

- Only 29% of those interviewed claimed to have read or heard about the efforts of US authorities to create a national system over the next few years.

- Notwithstanding this finding a solid majority were concerned about privacy and security in an EMR system. According to the survey:

  65% were very or somewhat concerned that computerization could increase rather than decrease medical errors.

  70% were very or somewhat concerned that sensitive medical information might be leaked because of weak data security.

  69% were very or somewhat concerned that there could be more sharing of medical information *without* patients knowledge.

  65% were very or somewhat concerned that some patients will *not* disclose sensitive but necessary information e.g. sexually transmitted diseases, treatment for alcohol or drug addiction or psychiatric illness, to doctors and other health care providers because of anxieties that the data will be entered in computerized records.

  69% were very or somewhat concerned that strong enough data security will *not* be installed in the new computer system.

[5] In 2004 the Bush Administration announced a new E-health initiative, which ensures that most Americans will have access to electronic medical records (EMR) within 10 years. In April 2004, a new Office of the National Coordinator for Health Information Technology was created and charged, among other things, with overseeing the successful implementation of EMR.

62% were very or somewhat concerned that existing federal health privacy rules protecting patient information will be relegated in the name of efficiency.

- The survey also found that respondents were evenly divided about the assertion that the benefits of EMR outweigh privacy risks: 48% accept that claim, while 47% reject it.[6]

There is no known comparable survey of community attitudes towards government proposals in Hong Kong to computerize, and centralize the keeping of, medical records of the entire population. In the absence of any such findings one is left to speculate. Nonetheless, the Health, Welfare and Food Bureau may wish to consider the commissioning of a baseline survey of public attitudes and perceptions towards proposals to establish a patient medical records database in Hong Kong. Such findings would offer some indication of the task that needs to be accomplished in order to build trust and confidence in the community. There can be little doubt that trust and confidence are a prerequisite for the broad based acceptance and future success of a computerized patient medical records database.

3.6 The PCO wishes to draw the attention of the Health, Welfare and Food Bureau to a Washington Post article titled, "Hacker Accesses Patient Records" (please refer to Appendix III). This incident is one of the most serious known security breaches of a medical records database. A hacker from the Netherlands[7] obtained access to confidential medical information at the University of Washington Medical Centre by using a sniffer programme to expose passwords. Once obtained, he assumed the identity of a legitimate computer user and accessed two databases

[6] Detailed findings of the study, "How the Public Sees Health Records and the EMR Program" can be viewed at: http://pandab.org/EHRrpt2-05.pdf.

[7] The hacker was allegedly motivated by a desire to publicize weaknesses in database security employed at the Medical Center rather than any desire to make money by selling the records on, most commonly to insurance and pharmaceutical companies. It is doubtful whether all hackers are driven by as 'benign' a motive.

containing 4,000 or more patient records in May and June of 2000.[8] Dated as this incident is, it would be imprudent to believe that in the intervening five years system security measures have become so impregnable that the possibility of such an event recurring is negligible. System security has made important strides in the past few years but these advances need to be set against the determination of hackers to expose system weaknesses and the sophistication of the methods engaged to achieve that goal. As indicated, the critical question is whether the majority of patients see the benefits of a computerized records system as outweighing the risks associated with it.

3.7 Although Hong Kong is not the USA there is no reason to suppose a similar incident could not happen here. On a network as open as that implied in the Discussion Paper, hundreds if not thousands of health care providers would be entrusted with passwords and protocols permitting access to patients' medical records contained in the database. More poignantly, given the limitations of current technology, it would not be possible for the Health, Welfare and Foods Bureau to *guarantee* total system security and that fact alone may heighten anxieties in the community. As is so often the case, the perception is the reality. Irrespective of how remote a system security breach may seem it is the public perception that such a breach *might* occur that is the issue under discussion. Perception management is something the Health, Welfare and Food Bureau will need to factor into their plans and a phenomenon worthy of being investigated in a baseline survey if the difficulties of managing a perceptual gap between the Bureau and the public are to be avoided.

3.8 In view of the anxieties that may be expressed the PCO recommends that the Heath, Welfare and Food Bureau conduct a Privacy Impact Assessment ("PIA") on any proposal that would involve the establishment of a computer-based medical records infrastructure that sought to retain patient records on one or more databases. The Commissioner feels that a PIA, similar to the one undertaken by the

[8] Full details of the incident as reported by the Washington Post can be viewed at: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contented=A46320-2000Dec8

Immigration Department,[9] prior to the launch of the Hong Kong smart identity card, would prove to be an indispensable and invaluable exercise in so far as the protection of personal data privacy is concerned. The more so as the database would contain a historical record of the individual's health data that far exceeds the volume of personal information contained in the chip on the Hong Kong Smart Identity card. In addition, the data contained on the identity card is considerably less sensitive than a detailed record of medical consultations, treatments, prescribed drugs and operations performed on the patient.

4 Privacy Impact Assessment and Privacy Compliance Audit

4.1 Privacy Impact Assessment is perhaps best thought of as the privacy equivalent of an environmental impact assessment. Essentially it is a systematic process that evaluates a project, proposal or new policy initiative in terms of its impact upon privacy. PIA has been gaining ground in terms of its acceptance since the 1990s and is now a mandatory requirement in some jurisdictions.[10] To be effective PIA needs to be an integral part of any project planning process rather than a casual afterthought. It is this mentality the PCO would encourage the Health, Welfare and Food Bureau to adopt prior to configuring a patient medical records database.

4.2 The natural extension of a PIA is a Privacy Compliance Audit ("PCA") which is a systematic and independent assurance process that seeks to elicit and evaluate evidence in order to verify whether the practices of a data user conform with clearly articulated privacy standards. In Hong Kong those standards would probably be benchmarked against the Ordinance. The Health, Welfare and Food Bureau might usefully conduct a PCA to ascertain whether data management practices

---

[9] Early in the planning stages of the smart identity card project senior officials at the Immigration Department consulted the Office of the Privacy Commissioner seeking advice regarding the perceived privacy issues of a smart card that would be carried by virtually the entire population. In due course the Immigration Department accepted the Commission's advice and appointed privacy consultants to undertake the PIA study.

[10] The Canadian government was the first national government to make PIAs mandatory. Canada requires all federal departments and agencies to perform PIAs for all programmes and services where privacy issues may be involved. Canada has adopted a PIA policy that provides a methodical framework for identifying and resolving privacy issues during the design or re-design of government programmes and services.

associated with a patient medical records database comply with the provisions of the Ordinance or fall short of those standards. Where the latter turns out to be the case the PCA would identify the deficiencies and indicate how any variance between benchmark practices and current practices may be eliminated.

4.3 A PIA may function as an early warning system that alerts the Health, Welfare and Food Bureau to the personal data privacy issues that a patient medical records database may give rise to. Experience indicates that a number of factors should be taken into account when conducting a PIA. The Health, Welfare and Food Bureau may wish to give consideration to these factors.

- PIA needs to commence at the very outset of any planning, project or policy initiative.

- The competencies necessary to perform a PIA on such an important proposal as a patient medical records database are unlikely to be found in a sub-committee that is delegated the task of evaluating the impact of the proposal on privacy. For this reason it is recommended that the PIA be conducted by external consultants with expertise in the field.

- An additional reason for appointing external consultants to conduct a PIA is that they lend impartiality to any investigation of privacy issues associated with setting up a patient medical records database. This is often an important aspect of ensuring public acceptance of the project and building trust and confidence in the system.

- Conducting a PIA should not however, be regarded as an end in itself. The report submitted by consultants should be measured in terms of the influence it exerts upon design details of the patient medical record database and the strategic decisions taken in conjunction with the launch of the system. The issues anticipated would relate to: system configuration; transmission and backend security measures; access protocols, audit trails; the transfer of patient medical record data; training and supervision of authorized system users etc.

5 Patient Medical Records Database Code of Practice

5.1 The PCO has been consistent in disseminating the view that, as far as personal data privacy and the application of the provisions of the Ordinance are concerned, what is illegal offline is illegal online. As a consequence the provisions of the Ordinance provide legal protection for all data subjects whose personal data is entered into a database. The most notable of these would be the protection of personal medical data from accidental or unauthorized use of that data. However, as indicated in the outline of the Data Protection Principles, issues such as consent, use, the transfer of data, access to and correction of data etc need to be taken into account and accommodated by the system.

One means of trying to signify the importance of the need to uphold the provisions of the Ordinance, insofar as they apply to medical data, would be for the Health, Welfare and Food Bureau, in consultation with a cross-section of health care providers, to give consideration to issuing a Code of Practice ("the Code") that offers comprehensive and specific guidelines for the practical guidance of all parties that have access to the database. A Code of Practice would need to be disseminated to those parties who should be required to attend and satisfactorily complete appropriate training programmes in the application of the Code.

The Commissioner recommends that the Health, Welfare and Food Bureau give consideration to the following matters which should be encompassed by the Code. These items give due recognition to the Data Protection Principles and fair information practices and have regard for the sensitivity of medical data.

- **Transparency**
  Patients who *consent* to their medical data being entered into a database should be explicitly informed in writing of their fundamental rights with regard to their medical data, what information the database will contain and how the medical data contained therein will be used.

- **Informed Consent**
  Apart from the primary use of medical data for clinical purposes (diagnosis, prognosis and treatment) all other uses and disclosure

of data should be subject to the prior and informed consent of the patient.

- **Security**
  Adequate security features should include appropriate systems architecture, security software, data encryption and operational protocols designed to prevent accidental or unauthorized access to, and disclosure of, patient's medical data in the database. The combined effect of these measures should help to ensure the confidentiality, integrity and accuracy of patient's records.

- **Right of Access to and Correction of Medical Records**
  Patients must be provided with the means to access and correct their data in the database as well as to be informed of the identities of third parties who have access their data and the purposes of permitting such access.

- **Sensitivity of Medical Data**
  It should be recognized that there are certain categories of medical data that are highly sensitive in nature e.g. medical data relating to sexually transmitted diseases, alcohol or drug addiction therapy and psychiatric disorders. The level of sensitivity of this medical data may require special recognition as a domain of absolute privacy or at least a domain with very stringent controls applied to it in terms of those having access to the data.

- **Accountability**
  Non-compliance with the provisions of the Code should be subject to appropriate sanctions and penalties. Non-compliance also suggests the need for appropriate supervisory controls and user auditing.

- **Public Responsibility**
  Exemptions to the Code should be clearly stipulated as the right to privacy is not absolute in that a balance should be struck between the personal data privacy rights of the patient, insofar as their medical data are concerned, and the collective rights of a society in relation to the public interest. These exemptions are usually related to the disclosure of data to support public health e.g. notifiable diseases, medical research, and to combat health

care fraud and abuse. In all circumstances the exemptions should be explicitly stated in the interests of transparency.

- **An Independent Monitoring Mechanism**
  A body, independent of the organizations or parties operating and accessing the patient medical records database, should have the ultimate responsibility of monitoring compliance with the Code. That authority should be invested with the power to investigate complaints and enforce any rulings that are the outcome of their investigations.

6 Concluding Comments

6.1 If the Health, Welfare and Food Bureau were to decide in favour of introducing a patient medical records database to be accessed by health care providers then the PCO would recommend that consideration be given to the following factors.

- Any medical records database and related IT infrastructure should comply with the provisions of the Ordinance and related Data Protection Principles insofar as patients' personal medical data are concerned. More specifically the Health, Welfare and Food Bureau should develop an E Privacy Policy Statement. This Statement should detail the Health, Welfare and Food Bureau's policies and practices in relation to the patient medical records database. Those policies and practices should cover the collection, holding and use of recorded medical data entered in the database. Under the provisions of the Ordinance data users are required to ensure that their policies and practices in respect of these matters can be readily ascertained by data subjects.

- The computer infrastructure and operating platform used to support the patient medical records database should be subject to rigorous reviews that seek to assess system security risks, personal data privacy risks and vulnerabilities associated with the system. The findings of successive reviews should be incorporated in E Security measures and operating protocols.

- The benefits derived from the patient medical records database in terms of its importance in facilitating clinical decisions, should be balanced against the potential risks arising from the accidental and unlawful accessing of patients' medical data.

- A Privacy Impact Assessment should be undertaken in conjunction with any decision in principle to develop a patient medical records database, *before* it becomes the subject of a more detailed policy proposal.

- If a more detailed policy proposal were to incorporate the establishment of a patient medical records database then the proper administration of that database would need to be subject to detailed procedures and protocols documented in user manuals. User manuals should be distributed to all persons authorized to access the system and fortified by programmes of induction and refresher training. In view of the sensitivity of medical data the PCO are of the view that that the principles outlined in section 5 of this submission be incorporated into a Code of Practice.

6.2 The PCO would like to express its appreciation for the opportunity to respond to this important discussion paper the subject of which is of considerable public interest. If the Health, Welfare and Food Bureau so wish the PCO is prepared to permit the views expressed in this submission to be cited in any further discussions on the matter. The PCO would also like to convey to the Health, Welfare and Food Bureau that its is most willing to discuss and expand upon the contents of this submission should that be deemed necessary. In addition, the PCO would welcome any opportunity to offer assistance to the Health Welfare and Food Bureau in the formulation of best personal data privacy practices relating to the configuration and operation of the patient medical record database and the drafting of a related Code of Practice.