# Executive Summary

1. Following a series of reported data loss incidents involving patient data, the HA Chief Executive announced the formation of the *HA Task Force on Patient Data Security and Privacy* on 5th May 2008 to conduct a review of HA's Personal Data System for the handling of patient data.

2. Its work was to be completed and a report submitted to the HA Chief Executive in three months. The Taskforce included members who are independent experts in the areas of privacy, computing and healthcare services:

| Membership of HA Task Force on Patient Data Security and Privacy | |
|---|---|
| Chairman: | Mr Stephen Lau, *former Privacy Commissioner for Personal Data* |
| Members: | Dr Chong Lap-chun, *Chairman of HA Clinical Data Policy Group* |
| | Mr Sunny Lee, *President of Hong Kong Computer Society* |
| | Mr Charles Mok, *HA Board Member, Chairman Internet Society Hong Kong* |

3. The Terms of Reference of the Taskforce are to:

- Review the clinical and operational requirements for exporting [downloading] of clinical data in the HA;
- Assess the mechanisms that are currently in place to protect the security and privacy of identifiable patient data; and
- Suggest improvements to these mechanisms to enhance patient data security and privacy in the HA.

4. The main approach used by the Taskforce has been to:

- Analyse the lessons learnt from the reported incidents, particularly those involving the downloading of clinical data, and assess the rectification measures already put in place - *Chapter 2;*
- Review the HA's overall Personal Data System for protecting identifiable patient data to identify opportunities for improvement - *Chapter 3*; and
- Based on these findings, to make recommendations to enhance patient data security and privacy in the HA – *Chapter 4*.

## Background

5. Following the reporting of a patient data loss case by the United Christian Hospital in April 2008, the HA undertook a look back and identified that there had been nine reports of loss of electronic devices which contained or might have contained patient identifiable data. Among them, eight cases had been reported to the police and seven cases were theft-related. The electronic devices lost included

four USB Flash Drives, one palm handheld device, one MP3 player, one desktop central processing unit (CPU), one laptop computer and one digital camera. The data lost had mainly been collected manually.

6. The day after the Taskforce was appointed, the loss of a mobile storage device possibly containing some 10,000 patient's identifiable data was reported lost by the Prince of Wales Hospital. This case involved a data download from a clinical system and use of a privately owned, unprotected USB Flash Drive.

7. In carrying out its work the Taskforce is aware of the resulting concerns about the possible inadequacies of HA's Personal Data System in protecting patient data and these cases provided a particular focus to our work.

## Overview

8. The protection of personal data is a responsibility of all organisations which handle such data. This is particularly applicable in healthcare organisations where substantial amounts of patient data are handled everyday and healthcare staff have a professional duty of care.

9. HA's adoption of new technologies has enabled sophisticated capabilities for the rapid and convenient sharing of patient information. This has contributed to important improvements in the quality of healthcare provided in our public hospitals, but it comes with attendant security and privacy risks to patient data.

10. Our review has shown that HA has over the years taken considerable steps to identify and address these risks. Structures, policies and guidance and training programmes, that collectively make up HA's Personal Data System for the protection of patient data, have been put in place. For example, in addition to the IT governance structure established within the HA Head Office (HAHO), each of the seven clusters within HA has a Clinical Data Privacy Committee and each hospital has an appointed Data Controller who is the subject officer for ensuring compliance with the Personal Data (Privacy) Ordinance (PDPO). Additionally, orientation programmes for new staff include elements covering information security and privacy.

11. There has also been early consideration of security and privacy as part of systems and process development. Moreover, technological measures have been established to control access to clinical systems and to protect HA's network from cyber-attacks, such as viruses, phishing, spam, and hacking.

12. Nevertheless, based on our assessments of the lessons to be learnt from the reported data loss incidents, and of HA's Personal Data System for the protection of patient data, we believe that more needs to be done to sustain and enhance the effectiveness of these measures. We have made 26 recommendations of specific actions to be taken in the areas of Policy (2), Structure and People (4), Procedures and Guidance (8) and Technology (12) that are designed to help HA continually improve its information security and privacy measures. These are summarised in Part II, and fully discussed in Chapter 4 of the Detailed Report. Additionally, our key overall findings are noted below under the following headings:

- Renewing and sustaining information security and privacy as a priority;
- Strengthening HA's Personal Data System;
- Raising and maintaining awareness of privacy risks; and
- Making greater use of technology to enforce safeguards.

## Key Findings

### *Renewing and Sustaining Information Security and Privacy as a Priority*

13. Renewing and increasing the visibility of HA's commitment to information security and privacy would help identify it as a clear priority. To help achieve this we have recommended the following measures:

    - A single HA-wide information security and privacy policy should be established and communicated to make it more accessible to all staff;
    - The role and strategic importance of information security and privacy should be clearly stated and expressly articulated and reinforced through the existing annual planning process at both the corporate and cluster levels;
    - Information security and privacy should be integrated into organisational performance objectives and for which Cluster Chief Executives should have an explicit accountability within their cluster and be required to make an Annual Information Security and Privacy Report; and
    - Dedicated resources should be allocated to the achievement of security and privacy objectives including the appointment of a Chief Information Security and Privacy Officer (CISPO) who should lead the HA-wide Information Security and Privacy programme driving forward improvements in a co-ordinated and integrated manner. It should be noted that information security and privacy is not solely an IT issue – it demands a comprehensive, strategic, team approach to finding effective solutions.

### *Strengthening HA's Personal Data System*

14. A good data handling system is one that has recognised the privacy risks, incorporated appropriate measures to mitigate these risks and that is capable of responding quickly to changes in the environment.

15. HA's Personal Data System for the handling and protection of patient data includes structure, processes, people and technology components. We have identified the following opportunities for further improvement in this system:

    - A HAHO committee should be established that has specific responsibility to oversight all HA-wide information security and privacy matters;
    - The cluster/hospital committee structures should be revisited to ensure a clear role and a specific focus on information security and privacy;

- The role and responsibilities of Data Controllers should be further defined, formally documented and communicated across HA;
- Guidance should be strengthened to require all HA projects that involve personal identifiable information to explicitly take account of the information/privacy policy and the principles established in the PDPO. Full Privacy Impact Assessment (PIA) is required for major projects with HA-wide or community-wide applications;
- HA's two access control policy directives, '*Patient under Care'* and '*Organisational need to know'*, should be made more explicit through the provision of additional guidance that aids consistent implementation;
- A mandatory three-step test should be applied before download privilege is approved in order to minimise downloading of identifiable patient data;
- Existing monitoring and audit arrangements should be rebuilt into a consolidated programme that is both structured and systematic to detect irregularities and monitor compliance; and
- Agreements with, and contractual obligations placed upon, relevant third parties (such as IT contractors, honorary appointees, researchers, confidential waste disposal contractors) who may have access to / handle patient data should be strengthened by ensuring the requirements of the PDPO are clearly incorporated.

***Raising and Maintaining Awareness of Privacy Risks***

16. HA's patient data users should be highly alert in handling sensitive or large quantities of personal data, both in paper and electronic forms. They need to be aware of the privacy risks in their everyday work and of the precautionary measures they need to take to protect patient data. The data loss incidents show that more needs to be done to raise and sustain awareness of privacy risks across HA.

17. To achieve this goal, HA needs to undertake proactive and regular privacy risk awareness raising measures. We have recommended that existing information security and privacy education/awareness raising measures should be developed into a more sustainable and integrated programme, which will help ensure staff apply information security policies and principles in their day-to-day roles and behaviours.

18. Maintaining a high penetration rate and measuring the effectiveness of this programme will also be important. An e-Learning training module, that utilises HA's existing platform, to be completed annually by staff and including performance assessment, would help to achieve this.

19. We are pleased to note that HA and the Office of the Privacy Commissioner for Personal Data will be jointly organising a *Patients' Data Privacy Campaign* with the objective of raising and sustaining awareness of privacy risks amongst healthcare staff.

### *Making Greater Use of Technology to Enforce Safeguards*

20. Throughout our review the Taskforce has been mindful of the need to make practical recommendations that can be adopted in the short-term to minimise the risk of any further loss of patient data. For this reason, we have made a significant number of additional technological recommendations that can be implemented across all HA hospitals within a shorter timeframe. These include: automatic encryption of downloaded data; whole disk encryption for portable electronic devices; physical restriction of the use of devices; and storage and sharing of data on secure file servers. In making these recommendations, we were mindful of the need to consider the complete lifecycle of the information that needs protection, and that they should directly address recognised risks and desirably have minimal impact on end users.

21. The Taskforce has also developed the following series of principles and an associated methodology for the ongoing enhancement of patient data protection:

- *Principle 1:* Minimise Access to and Use of Personally Identifiable Information*;*
- *Principle 2:* Minimise Transport of Personally Identifiable Information;
- *Principle 3:* Protect the systems containing Personally Identifiable Information from any external threats; and
- *Principle 4:* Provide concrete procedures and handling guidelines.

22. They can be applied to all circumstances in which patient data is accessed, can be used to guide technological and procedural efforts and are intended to be followed in order. The first two principles are intended to reduce the scope of risk to patient data. The second two are intended to mitigate the remaining risks. Based on these principles we have suggested additional security technologies suitable for deployment, where needed, throughout HA, including:

- Employing transparent encryption on all portable computing devices to automatically and securely protect stored data;
- Use of centrally managed, shared file servers to minimise the operational need to copy data to USB and other portable storage devices for ad hoc processing; and
- Deploying endpoint security enforcement that will control and limit the memory devices that can be used with HA systems and will automatically encrypt all data stored on the devices without requiring user action.

23. The selection and deployment of further technological security measures should be informed by the operational requirements and environments for patient data. Secure Information Workflow Reviews (Attachment 4) should be performed in accordance with the above *Four Principles* for this purpose.

24. Depending on the assessed level of risk, technologies can also be deployed and associated procedural guidelines promulgated to proactively strengthen user Identification and Authentication. This can help in controlling access to patient data and holding users accountable for its use.

25. Finally, it is important that HA should have a strategy to keep pace with the introduction of new information security technologies.

## The Way Forward

26. As noted above, we have made a significant number of technological recommendations that can be implemented across all HA hospitals within a shorter timeframe. With a view to the medium term we have also made recommendations chiefly aimed at strengthening the overall framework for information security and privacy. Work on this can start immediately, involving creating clear roles, revisiting and revitalising existing structures at both HAHO and cluster levels, to be followed by revamping the procedural guidelines and other documentation into a suitable form that meets the needs of different functions within the organisation and most importantly is accessible, informative and easily understood.

27. Most importantly, all of these aforementioned measures will need to be supported by a programme to raise and sustain awareness of data privacy and information security across HA. Undoubtedly, the incidents themselves, the publicity surrounding them and the actions taken by HA in response have all served to effectively heighten awareness amongst staff. Embedding a culture of data privacy and security that is 'second nature' will, undeniably, require ongoing efforts. To achieve this, we have made practical recommendations aimed at ensuring education and awareness raising programmes are given priority, that management visibly demonstrate its commitment to data security and privacy through both formal statements and informally in *executive walk-arounds* and that a sustainable system of awareness raising is implemented and continually updated based on feedback.

28. Electronic and paper records are equally important. Many of our comments and recommendations relate to both, but there are some elements of paper records that may warrant separate examination, in particular physical security.

## Acknowledgement

29. The Taskforce would like to express its appreciation to all who have supported, participated and contributed to this review, in particular members of the Health Informatics Unit, HA IT Services, Quality and Safety Division, Legal Services Section and Group Internal Audit.

30. As we have noted, many colleagues within HA have already put a great deal of effort into establishing policies, structures and systems for protecting personal data. This effort has been stepped up in recent months to develop and implement a number of the recommendations we have endorsed to effect system improvements. Implementing the rest of the recommendations will no doubt require sustained levels of commitment and hard work from colleagues across HA. The Taskforce acknowledges the significant contribution made by staff at all levels to securing the privacy of patient data.