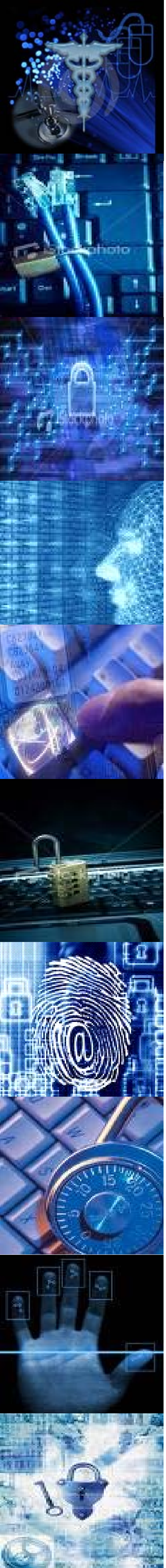


醫院管理局
HOSPITAL
AUTHORITY

Report of the Hospital Authority Taskforce on Patient Data Security and Privacy

August 2008

Contents

Executive Summary

1. Following a series of reported data loss incidents involving patient data, the Hospital Authority (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 within three months. The Taskforce’s membership includes 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, HA Clinical Data Policy Group*
	Mr Sunny Lee, *President, 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 of 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, make recommendations to enhance patient data security and privacy in the HA (*Chapter 4)*.

Background

5. Following a patient data loss incident reported by the United Christian Hospital in April 2008, the HA undertook a retrospective examination that identified there had been nine reports of loss of electronic devices which contained or might have contained patient identifiable data over the previous 12 months. Among them, eight had been reported to the police and seven 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 portable storage device possibly containing around 10,000 patient's identifiable data was reported lost by the Prince of Wales Hospital. This case involved data downloaded from a clinical system and the use of a personal, unprotected USB Flash Drive.

7. In carrying out its work, the Taskforce is aware of the resulting concerns about the possible inadequacies in HA's Personal Data System for protecting patient data and these reported data loss incidents therefore provided a specific focus.

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 every day 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 over the years HA has 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 while 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 risks as an important part of HA's systems and process developments. 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 made readily accessible to all staff;
- The role and strategic importance of information security and privacy should be clearly articulated and subsequently reinforced through the existing annual planning process at both corporate and cluster levels;
- Information security and privacy should be integrated into organisational performance objectives, 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, and be responsible for 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 prescribed 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 when handling such sensitive or large quantities of personal data, both in paper and electronic forms. They need to be well aware of the privacy risks in their every day work, as well as 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 information security and privacy risks across HA.

17. To achieve this goal, HA needs to undertake proactive and regular privacy risk awareness raising measures. We recommend 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 jointly organise 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 the 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 based 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 set 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 threats; and
- *Principle 4:* Provide concrete procedures and handling guidelines.

22. These principles 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 designed to mitigate the remaining risks. Based on these principles we have suggested additional security technologies suitable for deployment throughout HA, where needed, 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. For this purpose, secure Information Workflow Reviews (Attachment 4) should be performed in accordance with the above *Four Principles.*

24. Depending on the assessed level of risk, technologies can also be deployed and associated procedural guidelines promulgated as proactive measures to strengthen User Identification and Authentication. This can help control access to patient data and hold 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, to protect patient data, 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 and involves creating clear roles and revisiting existing structures related to information security and privacy at both HAHO and cluster levels. This should be followed by a revamp of 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 the aforementioned measures will need to be supported by a programme to raise and sustain awareness of information security and privacy 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.

II Summary of Recommendations

This section summarises our recommendations which are set out in more detail in *Chapter 4* of the *Detailed* Part of our report.

Policy

R1 *A single, clearly stated HA-wide Information Security and Privacy Policy should be developed, embedded HA-wide and made readily accessible*.

R2 *The role and strategic importance of information security and privacy should be clearly articulated and subsequently reinforced through the existing annual planning process at both corporate and cluster levels.*

Structure and People

R3 *To further enhance leadership and governance of information security and privacy, HA should:*

- ♦ *appoint a Chief Information Security and Privacy Officer (CISPO) who should report to a senior level and should lead the HA-wide Information Security and Privacy programme, and be responsible for driving forward improvements in a co-ordinated, integrated manner;*
- ♦ *establish a HAHO committee that has specific responsibility to oversight all HA-wide information security and privacy matters;*
- ♦ *revisit relevant cluster/hospital committee structures to ensure a clear role and a specific focus on information security and privacy with appropriate linkages; and*
- ♦ *further define, formally document and communicate the role and responsibilities of Data Controllers across HA. This should include explicit responsibility for the people-related aspects of information security and privacy such as education and training.*

R4 *Cluster Chief Executives (CCEs) should have an explicit accountability for information security and privacy within their cluster and should be required to make an Annual Information Security and Privacy Report to HAHO that includes:*

- ♦ *results of cluster-wide Information Security and Privacy risk assessment;*
- ♦ *continuous improvement measures taken; and*
- ♦ *Key Performance Indicators (KPIs) that demonstrate the effectiveness of their overall information security and privacy programme within the cluster.*

R5 *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, and would include:*

- ♦ *an information security and privacy workshops for staff covering a common component on overall policy and general data protection principles as per the PDPO, plus a tailored component targeting specific functional areas for the specific staff groups;*
- ♦ *an induction pack for new staff that includes greater emphasis and training on information security and privacy elements;*
- ♦ *an information security and privacy e-Learning refresher training module applicable to specific staff groups that reminds and updates staff about the risks and of their responsibilities and the professional duty of care, and includes a test, to be completed annually by all staff; and*
- ♦ *regular and planned use of all available channels to keep up staff awareness on information security and privacy.*

R6 *Increase the visibility of senior management in relation to information security and privacy by, for example, incorporating it as a prime element in regular executive walk-arounds. Each cluster could also undertake a periodic information security and privacy culture survey to help monitor the effectiveness of their awareness raising programme and to identify areas for further improvement.*

Procedures and Guidelines

R7 *Existing information security and privacy procedures and guidelines should be:*

- ♦ *redeveloped for different user groups, such as doctors, nurses, clerical staff, researchers, in simplified, easy to understand and more accessible form, that states in concrete terms what they should and should not do while pointing to where more detailed guidance can be found; and*
- ♦ *required to be regularly discussed in frontline teams - both its contents and how it will be applied in their work area.*

R8 *Strengthen guidance 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.*

R9 *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. Measures to make sure access privileges are reviewed on transfer and revoked on exit in a timely manner should also be enforced.*

R10 *Implement a mandatory three-step test before download privilege is approved to minimise downloading of patient identifiable data:*

- *Can this function be ceased or performed in another way?*
- *If no, can we modify the workflow in practical terms so downloading is not required?*
- *If no, can patient identifiers be removed or pseudo identifiers used?*

This three-step test should also be retrospectively applied to all existing approvals and at least every 12 months thereafter.

R11 *To reduce the potential for information security and privacy breaches, HA should renew its retention policy to ensure that personal data is not retained any longer than necessary, as required by PDPO Principle 2.*

R12 *Continue to encourage all staff to report incidents of unauthorised disclosure or loss of patient data in a timely manner through formal adoption of a just culture that differentiates between accidental loss and deliberate unauthorised access.*

R13 *Rebuild and resource existing monitoring and audit arrangements into a consolidated programme led by the CISPO that is structured, systematic and aligned to detect irregularities and monitor compliance with the PDPO and HA's policies and procedures, and includes:*

- *clear roles and responsibilities for devising audit strategies, conducting audits and providing HA-wide audit tools;*
- *reporting of results and taking corrective actions to improve measures as necessary; and*
- *continuous oversight, adjustment and improvement of the audit strategy to increase its cost-effectiveness.*

R14 *HAHO should further strengthen 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 by ensuring the requirements of the PDPO are clearly incorporated. A template for such agreements and contracts should be developed for common adoption. Also a planned programme of third party assurance in respect of these information security and privacy requirements should be initiated.*

Technology

R15 *All corporate IT systems should be urgently enhanced to automatically encrypt and password-protect downloaded identifiable patient data.*

R16 *Introduce, with immediate effect, the mandatory use of advanced USB Flash Drives with encryption and password 'lockdown' for protecting patient data.*

R17 *Upgrade the Advanced Incident Reporting System (AIRS) to better collect, highlight and report data loss incidents.*

R18 *HAHO should evaluate the operational requirements for the downloading of patient data from clinical systems and develop technological solutions to minimise this practice as much as possible. Where downloading is required, cost-effective protection technologies that are transparent to the users and commensurate with sensitivity of the data should be deployed.*

R19 *Transparent, whole disk encryption should be deployed on portable computing devices, such as laptop computers and PDAs, and on other computers at risk from theft.*

R20 *The use of centrally managed file servers as opposed to individual computers should be encouraged for storing patient data.*

R21 *Deploy 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.*

R22 *Computers containing patient data should be under the administration control of IT Departments and not the control of the computers' users.*

R23 *Comprehensive logging and reporting should be deployed to assist in detecting possible misuse of patient data by HA staff, IT administrators and external parties.*

R24 *Perform Secure Information Workflow Reviews in accordance with the Four Principles for Enhancing Patient Data Protection.*

R25 *Technologies should be deployed and associated procedural guidelines promulgated to proactively strengthen user Identification and Authentication (I&A) in support of controlling access to patient data and holding users accountable for its use. Measures should be commensurate with the threat environment.*

R26 *The CISPO, supported by HA IT Services, should be made aware of new technologies that are being considered for HA use and should keep pace with the introduction of new information security technologies and strategies.*

Chapter 1: Introduction and Background

1.1 Following a series of reported data loss incidents involving patient data, the HA Chief Executive (CE) 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. Its work was to be completed and a report submitted to the CE within three months.

Composition of the Taskforce

1.2 Members of the Taskforce were selected for their wide range of relevant experience and knowledge in their respective fields, which included information management, personal data privacy and hospital operations.

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, HA Clinical Data Policy Group*
	Mr Sunny Lee, *President, Hong Kong Computer Society*
	Mr Charles Mok, *HA Board Member,* *Chairman, Internet Society Hong Kong*

Terms of Reference

1.3 The Terms of Reference (ToR) given to the Taskforce are:

- ♦ Review the clinical and operational requirements for exporting [downloading] clinical data in the HA.
- ♦ Assess the mechanisms that are currently in place to protect the security and privacy of identifiable patient data. Mechanisms to be examined include:
  - policies & guidelines;
  - education & promulgation efforts;
  - system design & technical features; and
  - incident reporting & handling measures.
- ♦ Suggest improvements to these mechanisms to enhance patient data security and privacy in the HA.

Scope and Approach to the Taskforce's review

1.4 The main focus of the review has been on HA's Personal Data System for protecting identifiable patient data, including exporting of clinical data. Particular reference in this respect was given to the Data Protection Principles set out in the Personal Data (Privacy) Ordinance (PDPO) and, more specifically, Principle 4 - security of personal data:

> **Personal Data (Privacy) Ordinance - Principle 4 - security of personal data**
>
> *"All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorised or accidental access, processing, erasure or other use having particular regard to-*
>
> *(a) the kind of data and the harm that could result if any of those things should occur;*
>
> *(b) the physical location where the data are stored;*
>
> *(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;*
>
> *(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and*
>
> *(e) any measures taken for ensuring the secure transmission of the data."*

1.5 The Taskforce held nine meetings commencing on 7th May 2008. In addition to examining the reported data loss incidents, the Taskforce also carried out a wider review of HA's Personal Data System for handling patient data to identify opportunities for improvement.

1.6 The Taskforce has met with and received presentations from relevant subject officers within the HA. Additionally, the Taskforce has received and examined copies of the HA's information security and data protection policies, procedures and guidance, including but not limited to the following:

- ♦ Information Security Policy and Procedures Manual;
- ♦ Clinical Data Policy Manual;
- ♦ A Practical Guide to IT Security for Everyone Working in the HA; and
- ♦ Electronic Communications Policy.

1.7 In addition the Taskforce, through the HA, has obtained the services of an independent security and privacy consultant, Mr Thomas Parenty of Parenty Consulting, to assist in the work and provide expert advice. This work included further, more detailed analysis of the causes of the reported incidents, including direct interviews with a number of the staff involved, and examining HA's Personal Data System for handling patients' data to identify further opportunities for improvement.

Background to the Taskforce's review

1.8 The HA, since its establishment in 1990, has formulated strategies for the development of IT systems to automate its business processes to support both frontline patient care activities and back office administrative tasks. These various IT systems have been implemented in all HA's 41 hospitals / institutions and over 100 out-patient clinics. Within each hospital, clinical systems are utilised extensively in providing various services, including accident and emergency service, in-patient service, out-patient service, laboratory and pharmacy services, etc.

1.9 The clinical systems capture various data from patients during the provision of the above clinical services and share this patient information with other healthcare providers for healthcare related purposes. The daily workload of the major IT systems is outlined below:

Key statistics of the transaction workload of the major IT systems (2007/08)	
Clinical Management System (CMS) transactions	3,000,000 per day
Electronic Patient Record (ePR) transactions	500,000 per day
Patient Administration Systems (PAS) transactions	330,000 per day
No. of Patient records being accessed	90,000 per day
No. of clinical users accessing the clinical systems	12,000 users per day
Pathology test request transactions	38,600 per day
Dispensing transactions performed	122,000 per day

1.10 Following a patient data loss incident reported by the United Christian Hospital in April 2008, the HA undertook a retrospective examination that identified there had been nine reports of loss of electronic devices which contained or might have contained patient identifiable data over the previous 12 months. Among them, eight had been reported to the police and seven 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.

1.11 Expressing concern over the incidents, the HA Chief Executive, Mr Shane Solomon, appointed this Taskforce.

1.12 Subsequently, the Taskforce notes that further patient data loss incidents (both electronic and hardcopy) have been reported. On Tuesday 6th May 2008, for example, the Prince of Wales Hospital (PWH) reported the loss of a portable storage device possibly containing some 10,000 patient' s identifiable data referencing laboratory tests conducted. This case involved a data download and use of a USB Flash Drive. The staff member could not remember whether the file containing this data was deleted before it was lost.

1.13 It is estimated that a total of some 16,000 patients were involved in these cases. The data of about 3,000 patients did not contain any personal particulars while the data of around 2,000 patients was protected by password. HA has informed the affected patients through interviews, telephone calls or letters. To date there has not been any reported case of patient data leakage.

1.14 In carrying out its work, the Taskforce is aware of the resulting concerns about the possible inadequacies in HA' s Personal Data System for protecting patient data and these reported data loss incidents therefore provided a specific focus.

Chapter 2: The Incidents

2.1 Looking back at and analysing the root causes of past data loss incidents that have been reported within the HA has provided the Taskforce with evidence of areas that need improvement. Additionally, comparing the actions that have already been taken by the HA' s management to address these weaknesses with those the Taskforce would recommend has enabled any gaps and further action required, including longer term solutions, to be identified.

Summary of the data loss incidents

2.2 Table 1 (Attachment 1) summarises each of the ten reported electronic data loss incidents involving identifiable patient data over a period of some 13 months to 5th May 2008 when the Taskforce was appointed.

2.3 These incidents involved a range of portable electronic storage devices from laptops to digital cameras, however, half involved data stored on unprotected USB Flash Drives. The numbers of patients whose identifiable patient data was involved in each incident ranged from three to 10,000. Only two involved patient data downloaded from HA' s clinical systems; the others involved data collected / entered directly by the staff.

2.4 The taskforce understands that each of these incidents has been reported to the police and to the Privacy Commissioner, and all affected patients have been notified.

Analysis of the data loss incidents

2.5 Table 2 provides a summary analysis of these incidents:

Table 2: *Summary analysis of 10 electronic data loss incidents*

Incidents	1	2	3	4	5	6	7	8	9	10	Total
Purpose of data:											
♦ Operational					√	√				√	3
♦ Clinical		√	√	√	√		√	√	√		7
♦ Research	√					√	√				3
Use of data authorised	√	√	√	√	√	√	√	√	√	√	10
Password protected			√	√		√			part		3
Ownership of device:											
♦ HA			√	√	√	√					4
♦ Private	√	√					√	√	√	√	6
Loss due to:											
♦ Theft	√	√	√			√	√	√	√		7
♦ Accidental				√	√					√	3

2.6 In all cases the data was being used for an authorised purpose, seven cases the loss was due to theft, while in six cases a staff member's personal portable electronic storage device was used of which four were USB Flash Drives. Additionally where patient data was stored for research purposes, personal identifiers were included and were not password protected or encrypted in two of the three cases.

2.7 From this analysis, the following common factors were identified in these incidents:

- less than adequate security/privacy awareness/culture;
- less than adequate physical security;
- use of insecure methods of data storage / transfer;
- failure to adhere to requirements to use de-identified/pseudonymised data in conducting research; and
- use of own devices that did not have mandatory password or encryption.

The lessons learnt

2.8 As will be seen in Chapter 3, HA has a comprehensive array of policies and procedures for ensuring information security and privacy ranging from basic practical guidance to detailed instructions. They include the following relevant requirements:

- When accessing data for clinical research and education purposes, de-identified/pseudonymised data should be used as far as possible. (Clinical Data Policy Manual *(CDPM) section 3.1.1.2.2*)
- When the system generates downloadable or printed lists containing patient identifiers, patient data should always be de-identified as far as possible, such as using the patient key instead of HKID . (*CDPM section 3.4*)
- Appropriate measures must be taken to protect the security of the exported data, e.g. using encryption, or keeping the exported data safely in a secured area. (*CDPM section 3.5*)
- There is a pre-defined retention period and pre-imposed conditions for all exported data, including any copies. All such data should only be used in accordance with pre-imposed conditions and be destroyed once the pre-defined retention period expires. (*CDPM section 3.5*)

2.9 Strictly following these guidelines would likely have meant that the number of these reported losses due to theft and those incidents involving patient identifiable personal data should have been reduced.

2.10 Additionally, the guidance that was in place lacked sufficient specific attention to the use of USB Flash Drives to store patient data. The number of incidents related to the loss of a USB Flash Drives suggests that their use for this purpose has been increasing. Moreover, while HA has addressed the use of private laptops, by requiring their registration before they are to be used to process clinical data, similar requirements had not been established before privately owned USB Flash Drives could be similarly used. This suggests that more regular, proactive reviews are required to identify changing technologies that may introduce new risks.

2.11 The Taskforce's more detailed analysis of the PWH lost USB Flash Drive incident (following page) also showed that while a USB Flash Drive with encryption and password protection would mitigate the risk of patient data disclosure due to its loss or theft, examining the workflow may enable possible solutions to protect sensitive data to be developed without imposing additional security responsibilities on staff.

2.12 Additionally, the Taskforce believes that these incidents indicate that consideration should be given to implementing further technological solutions for data protection that are transparent to the users, where possible, as well as relying on staff's appropriate behaviour to ensure security of data.

2.13 A number of these incidents, at least initially, were reported and treated as the loss of low value assets rather than the loss of patient data. Without appropriate recognition, and timely reporting and escalation to the relevant subject officers, the valuable learning opportunity can be easily lost and remedial measures taken less optimally effective. It also suggests that management sensitivity to the possible impact of such losses needs to be greater.

2.14 These incidents also highlight the importance, and suggest a possible prevailing lack, of appropriate mindset by individual staff towards information security and privacy when handling patient data.

Analysis of the PWH Lost USB Flash Drive incident

A USB Flash Drive, possibly containing patient data, was lost in a taxi. The patient data included Hong Kong ID, name, lab test title, request location & unit, test request date, authorisation date, and unit price. The USB Flash Drive belonged to the employee who was working on this patient data and did not have password or encryption protection. An initial assessment points to a lack of security awareness, as well as lack of physical and technological protection for the USB Flash Drive and its contents.

The use of a USB Flash Drive with encryption and password protection would mitigate the risk of patient data disclosure due to a lost or stolen USB Flash Drive, but it is informative to examine why the patient data was copied onto the USB Flash Drive in the first place and what measures could be taken to avoid this practice.

The clerical staff who lost the USB Flash Drive works in the Pathology Department at Prince of Wales Hospital (PWH) and was working on the preparation of worksheets that would be used for inter-hospital, cross-charge billing for tests performed at PWH. Most requests for tests are entered into the Laboratory Information System (LIS). This test information is then exported to a web-based Decision Support System (DSS) from which it can be downloaded in the form of Excel worksheets. The information that is downloaded from the DSS is grouped by laboratories, but the billing is done by hospital so the clerical staff's task was to regroup the test information by hospital. Since the clerical staff did not have Excel installed on her computer she copied the data onto a USB Flash Drive to copy it to a colleague's computer that did have Excel so she could do her work.

If the clerical staff had Excel installed on her computer there would have been no need for copying data onto the USB Flash Drive and the opportunity for unauthorised disclosure of patient data via a lost or stolen USB Flash Drive would have been eliminated. It was explained that the Cluster IT department discouraged the widespread installation of the 'Office' software for security reasons though those security reasons were not articulated by management nor through a written policy. Further analysis shows that this entire task could have been eliminated if the DSS exported test information had been grouped by hospital instead of laboratory.

In the aftermath of the incident, the Office software was installed on the clerical staff's computer, and based on discussions during Task Force-sponsored interviews, the Business Manager of the Pathology Department is considering requesting a change in the DSS so that exported test information will be categorised by hospital. These changes are in keeping with the principle of minimising the transport of personally identifiable information and obviate the risk that led to the patient data loss in this incident without imposing additional security responsibilities on staff. By examining workflow it is often possible to develop solutions to protect sensitive data with little or no impact on end users.

Remedial actions taken since these incidents

2.15 Key actions already taken by the HA management since the incidents to reduce the risk of further data loss involving portable electronic storage devices include:

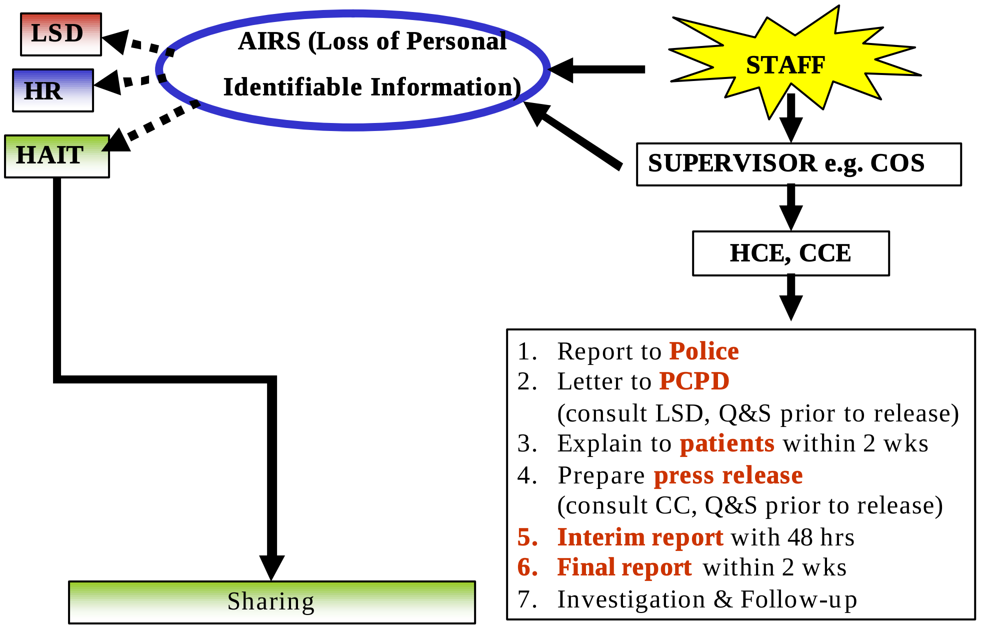
- ♦ An immediate e-mail from the HA Chief Executive to all HA staff, stating that:
  - export of identifiable personal data is not allowed unless absolutely necessary for patient care;
  - any portable electronic devices containing identifiable patient data must be kept in a secure environment;
  - all electronic files containing patients' identifiable personal data must be encrypted and password protected; and
  - no staff may remove USB Flash Drives which contain identifiable personal data from the hospital, except with the written permission of the Hospital Chief Executive (HCE).
- ♦ Through various channels all HA staff were reminded to be more aware of the need to protect patient data.
- ♦ Advanced USB Flash Drives with encryption and password lockdown features were introduced for use since 13 May 2008.
- ♦ A Circular on "Enhanced Measures on Enforcing Personal Data Security" was issued on 14 May 2008, stating that:
  - export of identifiable personal data (i.e. containing HKID and/or name) to portable electronic devices was prohibited unless using Secure USB Flash Drives provided by HA;
  - any device containing identifiable patient data must be kept in a secure environment;
  - all files with identifiable personal data, whether exported or manually created on PCs, removable storage devices and other portable computing devices, must be encrypted and password protected;
  - all files with identifiable personal data previously downloaded on PCs, removable storage devices or other portable computing devices which are not encrypted and password protected must be deleted immediately; and
  - no files with identifiable personal data should be downloaded, copied or stored in staff owned PCs, removable storage devices, such as USB Flash Drive and other portable computing devices such as notebook, PDA or smartphone.
- ♦ Corporate clinical systems were urgently enhanced so that all identifiable personal data downloaded is encrypted and password protected - implemented with effect from midnight 14 May 2008.

2.16 Actions have also been taken to improve reporting of data loss incidents: containment management once a data loss has been reported; and ensuring the lessons are learnt, including:

- Policy on the management of loss of electronic devices containing patient identifiable personal data was issued on 15 May 2008 that required:
  - staff to immediately report to their supervisor and through HA's Advanced Incident Reporting System (AIRS) the loss of electronic storage devices carrying patient data with details such as the storage device, the date, the place of loss and the type and quantity of patients' data involved; and
  - a report to HAHO within 48 hours, as well as a report to the Privacy Commissioner and inform the relevant patients within two weeks.

- These requirements are summarised in the following flowchart:

Loss of electronic devices with personal data



1. Report to **Police**
2. Letter to **PCPD**
   (consult LSD, Q&S prior to release)
3. Explain to **patients** within 2 wks
4. Prepare **press release**
   (consult CC, Q&S prior to release)
5. **Interim report** with 48 hrs
6. **Final report** within 2 wks
7. Investigation & Follow-up

- The Advanced Incident Reporting System (AIRS) has also been upgraded from 20 May 2008 to better highlight and report such data loss incidents. This includes a new reporting category of '*Loss of personal identifiable information*" and collection of relevant information, including remedial actions taken.

2.17 The Taskforce notes that several of these measures were already underway before these incidents were reported, particularly the acquisition and implementation of USB Flash Drives with encryption and password lockdown features.

Planned further enhancement measures

2.18 In addition to establishing this Taskforce, HA has also already commenced the following:

- An urgent review of the necessity for all downloading of identifiable patient data with a view to:
  - minimising such requirements; and
  - where required, ensuring they are subject to strict technical and procedural safeguards.
- An HA-wide awareness raising programme designed particularly to explain and reinforce the new measures noted above and with forums in all main hospitals. This programme commenced in the United Christian Hospital on the 19 May 2008, followed by Ruttonjee and Tang Shiu Kin Hospitals on 20 May 2008 and has already been completed in 13 hospitals across HA.
- A promotional video on protecting patient data has been developed and broadcast on HAChannel and planning is in progress to introduce refresher education programs to HA staff on protecting patient data.

What more needs to be done?

2.19 The Taskforce welcomes these measures that have now been implemented since the incidents became known or are already underway. Technological Strategies for Protecting Patient Data are shown in Attachment 2.

2.20 To assist in further improvement, the Taskforce has developed a set of principles and an associated methodology for the ongoing enhancement of patient data protection. These have, in turn, led to the selection of additional security technologies suitable for deployment, where needed, throughout HA.

2.21 Additionally, the Taskforce wishes to note (Attachment 3) that there are different types of unauthorised disclosure of patient data and the importance of the response to incidents of each type. Other ongoing measures required, such as steps to increase information security and privacy awareness amongst HA staff, are addressed in Chapter 3.

Four Principles for Enhancing Patient Data Protection

2.22 Based on an analysis of the data loss incidents as well as a review of HA's management and use of patient data, the following principles were developed to enhance patient data protection. They can be applied in all circumstances in which patient data is accessed and can be used to guide technological and procedural efforts. The principles are intended to be followed in order. The first two are designed to reduce the scope of risks to patient data, whereas the later two are designed to mitigate the remaining risks.

Principle 1: Minimise Access to and Use of Personally Identifiable Information (PII)

2.23 Patient data can be considered to consist of two components. The first is medical information relating to a patient. This could include medical test results, X-rays, and doctors' notes. The second is identifying information, viz. Hong Kong ID, Chinese and English names, that link this medical information to a specific individual. The Personal Data (Privacy) Ordinance (PDPO) governs all aspects of the creation, use and disposal of patient data when these two components are combined. Clinical information that cannot be identified as belonging to an individual does not fall under the definition of personal data as per the PDPO.

2.24 The need to keep both components together depends on the context in which the patient data is being used. In a clinical environment in which a patient is currently under care, unambiguous identification of a patient is critical to ensure proper treatment. In the context of a clinical audit, it is also necessary to maintain the linkage between a patient's medical information and identity. Performing research, on the other hand, does not require a patient's identity. In some cases, it may be necessary to link multiple medical records belonging to an individual, but it is not necessary to know that individual's identity.

2.25 Minimising access to and use of personally identifiable patient data needs to be applied at all stages of the data's lifecycle, including creation. In order to be able to separate medical from identifying patient data, it is first necessary to ensure that identifying information is not included in the medical information component. For example, a photo of a patient should not have identifying information, such as a gum label, in the photo itself. An alternate approach could be to include identifying information in the file name of the photo or to otherwise logically associate the photo with a patient's record. This could be changed later if the photo is no longer needed for clinical use, but still has utility for research or teaching purposes.

2.26 While it is not always possible to know a priori the purpose for which patient data is being accessed, application functions that print or download patient data into a file should be examined to determine if the patient identifying information is operationally required. If not, the application should be modified so that the identifying information is not included or an anonymous identifier is used instead.

Principle 2: Minimise Transport of PII

2.27 The risk of unauthorised disclosure of patient data increases with the number of computing devices on which the patient data is stored. There is the potential for disclosure while the information is stored on a computing device as well as when being transported between computing devices. While different mechanisms, such as email or USB Flash Drives, may be used for transporting information, they all have vulnerabilities that could put patient data at risk.

2.28 There are two primary motivations for transporting PII: (i) to facilitate an individual's work; and (ii) to share information among HA colleagues. Scenarios in which patient data is currently being transported should be examined to determine if alternatives are possible that eliminate the need for transporting. Drawing from lessons learned from the above previously incidents, transporting of patient data can be eliminated in some cases if staff have the software necessary to perform their tasks installed on their computers. The transporting of patient data in a collaborative context can be avoided, for example, if the data is stored on a shared server.

Principle 3: Protect Environments with PII

2.29 All the incidents of potential disclosure of patient data involved the loss or theft of computing devices or devices with electronic storage. Encryption is the standard technological approach to mitigate this type of physical security threat. If the patient data cannot be decrypted then the loss of a device with such data is an equipment loss, not a potential disclosure of patient data.

2.30 Encryption does not solve the problem of protecting patient data; rather, it reduces the problem from one of protecting patient data to one of protecting the key used to encrypt the data. In practice, these encryption keys are often generated from passwords which are easier for users to remember. Encryption under user control can adequately address the risks present in all of the incidents, but it does so through an additional security burden for users. Every security-relevant action a user makes is a potential vulnerability because the user could perform the action incorrectly. To the degree possible, encryption should be deployed in a manner that is transparent to users. This both enhances the level of protection and eases the burden on users.

2.31 Looking beyond the immediate causes of the incidents, creating a protective environment for PII involves protecting the systems containing PII from any external threats, ensuring that users only have access to the patient data they need to do their job, and to the degree possible, are constrained so that they only use that data for its intended purpose.

2.32 A necessary pre-condition for all of these protection measures is that all devices that contain patient data have to be under HA administrative control. From a pragmatic perspective this means that HA needs to provide staff with the devices required to do their jobs effectively.

Principle 4: Provide concrete handling guidelines

2.33 The HA has published a significant number of information security and privacy policies, standards, guidelines and training materials that cover a wide range of topics. In addition, these materials reference external directives, such as the PDPO. A full reading of all these materials by all HA staff is neither possible nor necessary. The security and privacy responsibilities facing individual staff are much more specific and are better addressed through guidelines that are customised for their specific job functions.

2.34 This can be accomplished by reviewing their work responsibilities, tasks, appropriate access to patient data and use of IT systems. This will identify the security-relevant actions they make. This set of actions should have been minimised through application of the previous principle of protecting environments with PII. The body of HA security materials can then be drawn upon to create actionable guidelines. An essential property of these guidelines should be that they make it easy for staff to know what they need to do in order to protect patient data.

Further technological security solutions

Secure Information Workflow Methodology

2.35 The application of the Secure Information Workflow Methodology (Attachment 4) involves the selection and use of technology to either eliminate situations in which patient data may be prone to be lost or stolen; or if that is not possible, to mitigate the risks of such possibilities. The selection of these security technologies:

- ♦ takes into account the complete lifecycle of the information that needs protection;
- ♦ directly addresses the recognised risks; and
- ♦ minimises the impact on end users.

Alternative patient identifiers

2.36 Within the HA' s Clinical Management System (CMS) there is a unique identifier associated with each patient. This is used for internal processing, is never exported outside of the application, and therefore is never visible to CMS users. Calculating a secure hash function, also known as a message digest, on this identifier will result in another unique number that could be used in place of the HKID to identify records as belonging to an individual without revealing that individual' s identity.

2.37 Secure hash functions, e.g. SHA-1 and MD5, have three properties that are relevant to this discussion. The first is that no two inputs, viz. the internal CMS patient identifier, will "hash" to the same value. This means that there is no possibility that records belonging to one patient could be construed to belong to another. This helps ensure the integrity of medical research where it is necessary to correlate different medical records belonging to the same patient.

2.38 The second property is that it is computationally not feasible to derive the original identifier from the hash value. This means that it is impossible for someone who has an anonymous hash value identifier to find out the corresponding patient' s real identity.

2.39 The third property is that, unlike symmetric and asymmetric encryption, hash functions do not require the use of an encryption key. This simplifies both the development of the solution within CMS and other applications that utilise HKID as well as the deployment of the solution because there are no keys to manage. Further, encrypting HKIDs would not be as strong a solution since decryption would reveal the HKIDs.

Encryption of portable computing device

2.40 Encryption is the technology of choice to protect stored data, e.g. files, on a portable computing device, such as a laptop, PDA, or Smartphone, that may be lost or stolen. The encryption may be applied to the device' s entire hard disk or may be applied on a file or directory basis.

2.41 In the context of the incidents and the HA' s overall operations, "whole disk" encryption is preferred over file or directory encryption. The first reason is that it provides protection for all of the sensitive or confidential information on the device without requiring the user to make any determination as to what should be protected or not. Secondly, whole disk encryption can be linked to the operating system, e.g., Windows, login process, so that users do not have to change the way they use their computers. Thirdly, many whole disk encryption products include support for a corporate key recovery function so that access to encrypted data is possible even if the laptop' s user is not available. If physical control over desktop computers cannot be guaranteed, as was the situation in Case #6 (Attachment 1), then whole disk encryption should be considered for them as well.

2.42 The encryption of individual files for transfer between computers may be called for if an alternative, secure means is not available. The 128-bit, RC4 encryption that is available within Office applications is suitable for this use. A 128-bit key is resistant to *brute force* attack and the reported vulnerabilities in the Office use of RC4 cannot be exploited if an attacker only has one copy of an encrypted file. The key used to encrypt a file needs to be communicated between the sender and recipient in a secure manner. In practice, this means that the password used to generate the key should be sent "out of band" from the method used to transfer the file. Mobile phone SMS or oral communication are acceptable methods.

Use of centrally managed, shared file servers

2.43 One of the common operational needs that leads to the copying of patient data on to portable memory devices, such as USB Flash Drives, is the sharing of data with colleagues. In many cases, this type of sharing can be supported through the alternate use of centrally managed, shared file servers. Providing a centralised facility where colleagues can access patient data eliminates not only the need for portable memory devices to transmit this data but also email. In order for this approach to be effective it is necessary to assign someone the responsibility for determining and configuring access control permissions for the data on the file server and to ensure that any remote network access to the file server is protected.

2.44 Storing information on a file server is also an alternative to storing information on staff PCs or laptops. In addition to the security benefits resulting from minimising the number of computers on which patient data is stored, this approach simplifies administrative tasks such as back-up and recovery. Further, it makes secure, viz. encrypted, provision of back-up easier.

2.45 Providing a shared file server does not, by itself, prevent a user from downloading information from the server onto a computer. The use of desktop virtualisation technology within HA may be expanded to address this situation. This technology can be used in such a way that, when a user is accessing a shared server, he does not have access to the local computer' s disk and so cannot download any information to it.

Controlling use of and protecting data on portable memory devices

2.46 While the use of portable memory devices, such as USB Flash Drives and MP3 players can be minimised, there are several options for addressing situations in which their use cannot be eliminated. The most expeditious approach is to employ USB Flash Drives with built-in encryption, such as Kingston' s Data Traveler Vault Privacy, which has already been deployed by HA. This addresses the specific risk scenarios found in the incidents.

2.47 A more comprehensive approach addresses additional risks that arise from the use of portable memory devices as well as addressing ease of use. Products within the endpoint security market target these issues. Portable memory devices pose two types of risk to the HA. The first is their, usually unintentional, use as a means of introducing viruses and other malware into HA systems through infected files. The second is their role in the unauthorised disclosure of patient data through their loss or theft. The first type of risk can be addressed through the registration of portable memory devices that are authorised to be connected to HA computers and whose contents are scanned for viruses and malware at the time of connection. This mitigates the risk from use of non-HA approved portable memory devices.

2.48 The second risk can be addressed through encryption of the data being copied to the memory device. This encryption can be performed transparently to the user and can be configured so that the data can only be decrypted on another HA computer. This addresses the risk of data disclosure without imposing an additional security burden, such as remembering another password, on the end user. It also prevents the unauthorised copying, via portable memory device, of patient data from HA computers to non-HA computers.

2.49 This solution does require the installation of endpoint security software on all of the " open" PCs and laptops that have operative USB ports, and its ongoing effectiveness requires that a computer' s user cannot uninstall the software at a later point. This is one of the reasons why all HA end user computers have to be under the administrative control of the relevant IT department and why end users cannot have accounts with administrative privileges.

Chapter 3: The HA's Personal Data System

3.1 While Chapter 2 looked at the lessons from reported incidents, this Chapter sets out the results of the Taskforce's assessment of the overall measures (*the Personal Data System*) put in place by HA to protect patient data against unauthorised or accidental access, processing, erasure or other use under the following categories:

- ♦ Identification of information security and privacy risks; and
- ♦ HA's Personal Data System to protect patient data – Structure, Process, People and Technology.

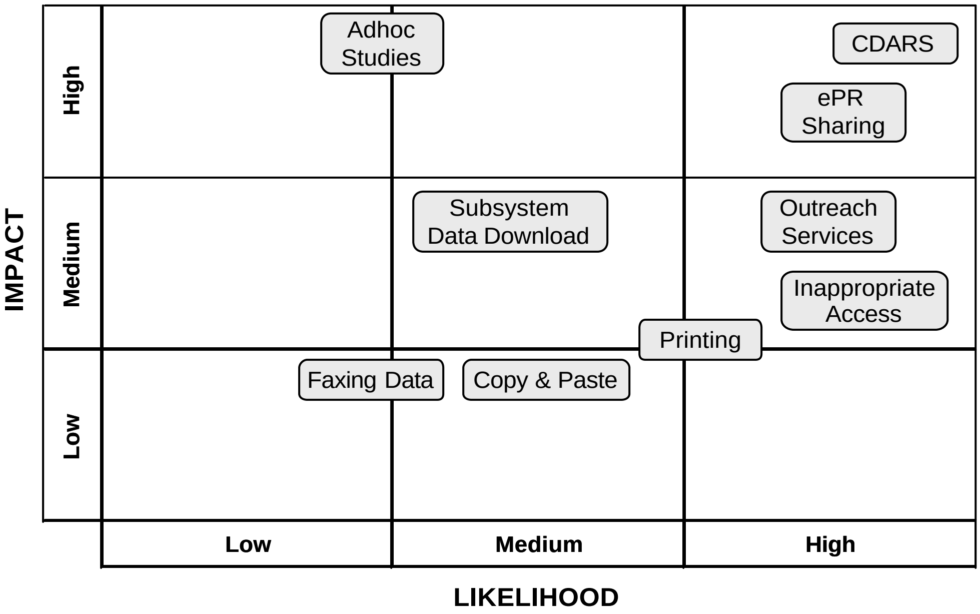
3.2 A good data handling system is one that has recognised the risks, then incorporated appropriate measures to mitigate these risks and is capable of responding quickly to changes in the environment. These measures would include both hard (e.g. access controls, technology) and soft (e.g. culture) controls.

Identification of information security and privacy risks

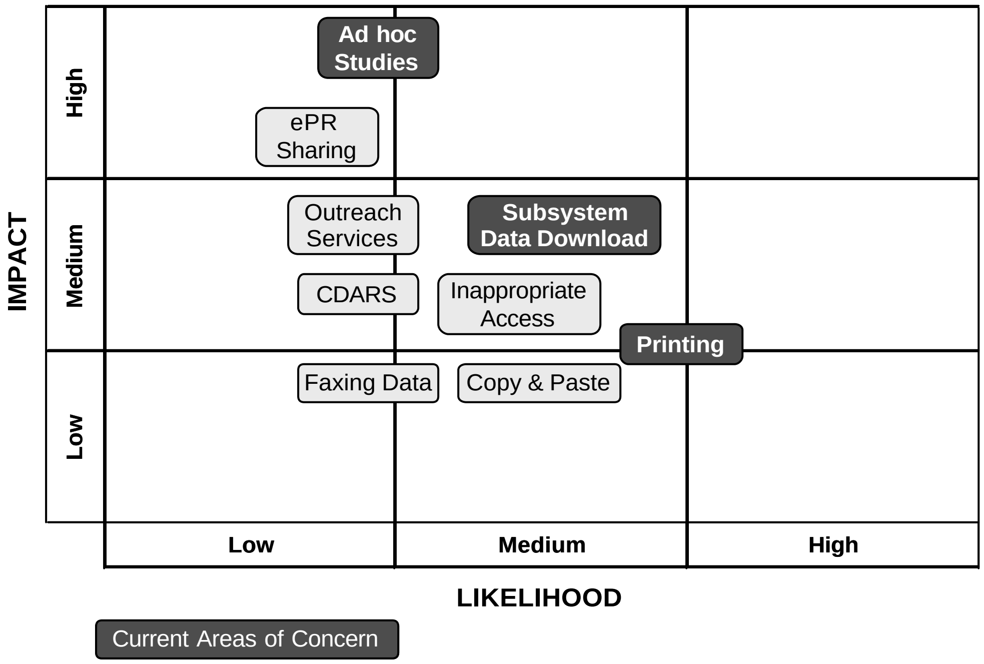
3.3 The Taskforce was advised that HA's IT Department carries out a macro level risk assessment each year as part of its annual planning process and that the results are presented to the IT Governing Committee (ITGC) and the HA Board Audit Committee. "Breach of confidentiality" was identified as being of increasing risk in the latest assessment (February 2008) as a result of projects such as ePR–sharing.

3.4 This was supported by the following two risk assessment matrices showing: the *Inherent Data Security and Privacy Risks (Matrix 1)* - due to the nature of the business and before risk mitigation measures; and *Residual Risks* (Matrix 2) – after current mitigation measures.

Matrix 1: RISK BASED APPROACH TO DATA SECURITY AND PRIVACY - INHERENT RISKS -

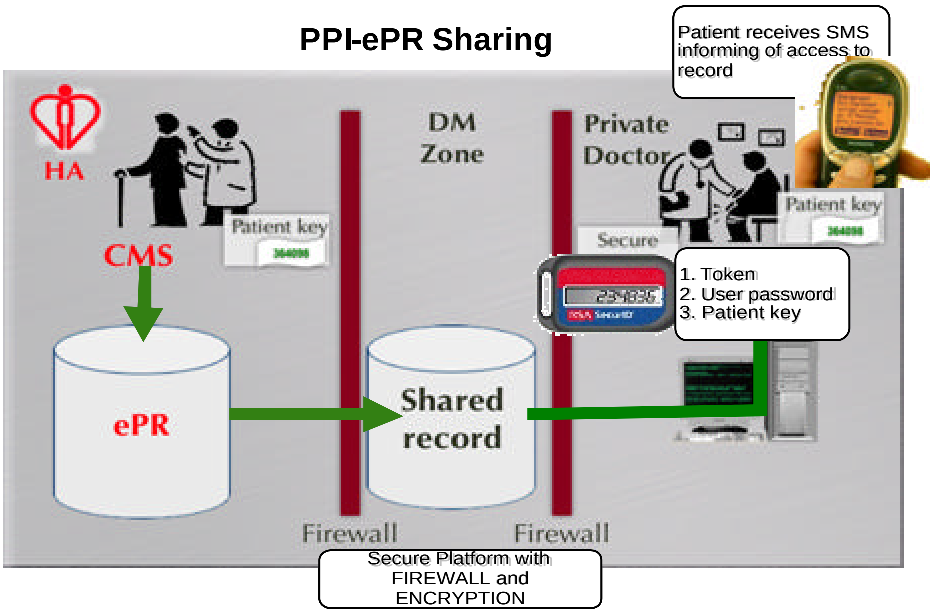


Matrix 2: RISK BASED APPROACH TO DATA SECURITY AND PRIVACY - CURRENT RESIDUAL RISKS -



3.5 The Taskforce notes that mitigation measures put in place have decreased all higher inherent risk concerns, as shown from Matrix 1 to Matrix 2. The Taskforce also notes that "Subsystem download" had been identified as an area requiring attention. However, it is also noted that individual staff manually entering and copying patient data to portable electronic devices were not identified as a risk. This suggests that such risk assessments need to be broader that just IT risk, plus need to be on an enterprise-wide basis and include both electronic and paper based information.

3.6 By way of example, the following chart shows the key measures put in place to decrease inherent information security and privacy risks associated with ePR-sharing. The Taskforce notes that the Privacy Commissioner's office was involved in the development of these measures.



HA’s Personal Data System to protect patient data

3.7 The volume and sensitivity of patient data held by the HA reaffirms the need and importance of achieving a consistent and high level of *information security and privacy.* The Taskforce considers that this has been recognised by the HA and is demonstrated by its endeavours to establish an adequate Personal Data System for the protection of its patient data while also balancing operational requirements. This system comprises structure, process, people and technology components.

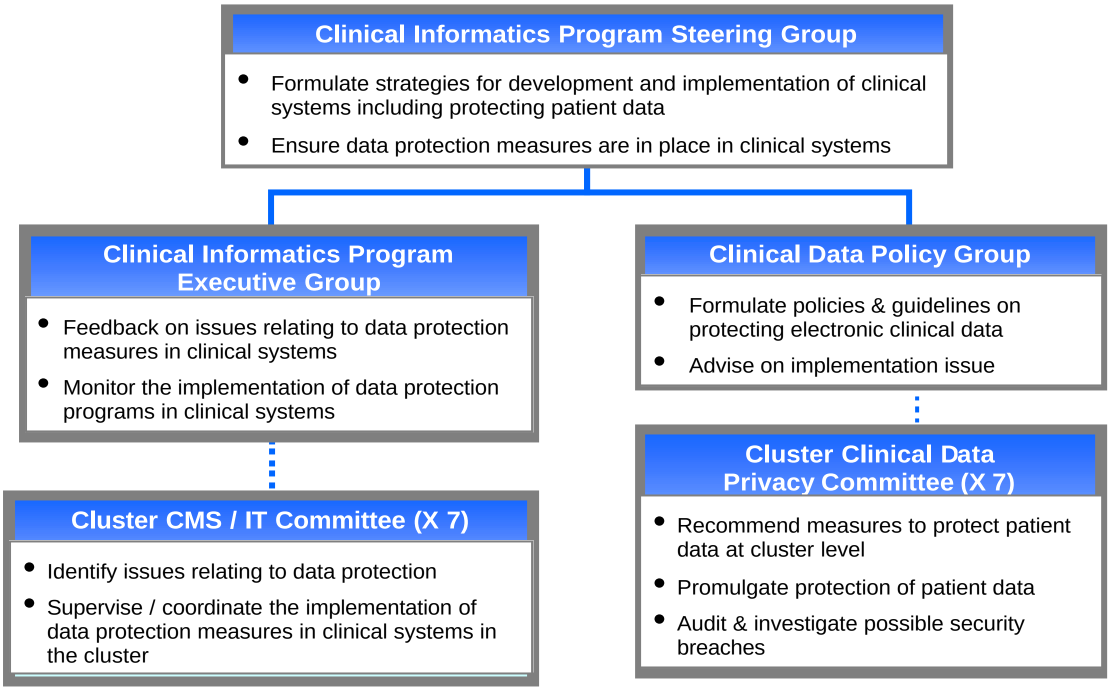
3.8 However, our assessment suggests that more can to be done, particularly if these endeavours are to be sustained and remain effective in the changing environment. It must be remembered that the strength of the system is only as good as its weakest link.

Structure

Roles and Responsibilities

3.9 HA has established a committee structure whose Terms of Reference include (as shown in chart below):

- ♦ Formulating strategies, policies and guidelines for protecting patient data;
- ♦ Supervising/coordinating the implementation of data protection measures; and
- ♦ Monitoring the implementation of data protection programmes in clinical systems.



Clinical Informatics Program Steering Group

- Formulate strategies for development and implementation of clinical systems including protecting patient data
- Ensure data protection measures are in place in clinical systems

Clinical Informatics Program Executive Group

- Feedback on issues relating to data protection measures in clinical systems
- Monitor the implementation of data protection programs in clinical systems

Cluster CMS / IT Committee (X 7)

- Identify issues relating to data protection
- Supervise / coordinate the implementation of data protection measures in clinical systems in the cluster

Clinical Data Policy Group

- Formulate policies & guidelines on protecting electronic clinical data
- Advise on implementation issue

Cluster Clinical Data Privacy Committee (X 7)

- Recommend measures to protect patient data at cluster level
- Promulgate protection of patient data
- Audit & investigate possible security breaches

3.10 The Taskforce notes that of these, only the Cluster Clinical Data Privacy

Committees are solely focused on information security and privacy. In each of the others, information security and privacy is just one part of their respective Terms of Reference.

3.11 At the HA Head Office (HAHO) level, no single post has overall responsibility for leading on information security and privacy, although we understand such a post has been considered. The Taskforce strongly supports the establishment of such a dedicated post to lead, co-ordinate and monitor this programme. A single governance committee whose Terms of Reference either solely or materially focus on information security and privacy should also be considered to provide a sharper focus.

3.12 Additionally, at the cluster level the number of committees that have a role in information security and privacy (Cluster Clinical Data Privacy committee, Cluster CMS / IT committee, Cluster Clinical Research committee, Cluster Medical Records committee) can potentially lead to overlaps and inconsistent practices. Revisiting these established governance structures and revising their Terms of Reference to more specifically focus on information security and privacy would allow these data protection measures to be further strengthened.

Data Controller

3.13 Additionally, as part of its overall responsibility/accountability structure, HA has put in place a legal compliance framework that includes appointed subject officers at the HAHO and hospital levels. These subject officers, known as Data Controllers, are responsible for assuring compliance with the Personal Data (Privacy) Ordinance (PDPO) across HA.

3.14 The stated roles of these designated Data Controllers are relatively narrow. While being the subject officer for the PDPO, they often can have limited other involvement in the information security and privacy matters in their respective hospital. Broadening their responsibility to include co-ordinating measures to protect personal data privacy across the hospital, such as information security and privacy education and awareness raising, would enable them to be more visible and play an enhanced role.

Accountability

3.15 Under HA's decentralised management structure, Cluster Chief Executives (CCE) are accountable for the operations of their cluster, including legal compliance. While we understand that there are more than 60 Ordinances which are relevant to HA, the Taskforce is of the view that each CCE should be held explicitly accountable for information security and privacy matters within their cluster because of their importance and sensitivity.

3.16 This could be achieved by inclusion of this accountability within each CCE's job description and through the requirement for an *Annual Information Security and Privacy Report.* This report would include Key Performance Indicators (KPIs) that demonstrate the performance of the cluster in information security and privacy matters, as well as agreed annual plan target achievement.

Process

3.17 HA has developed a comprehensive range of policies, guidelines and instructions relating to the collection, use and security of patient data. These are communicated through a series of manuals and handbooks, ranging from simple guidance, such as *dos and don'ts* for frontline staff, to more detailed coverage for subject officers and those who need to know more, including:

- A Practical Guide to IT Security for Everyone Working in the Hospital Authority.
- Clinical Data Policy Manual, which mainly governs the ownership, access, disclosure and use of patient data.
- Information Security Policy and Procedure Manual, which includes sections on: removable computer media; disposal of media; security of media in transit; and data encryption – all relevant to the use of portable electronic storage media.
- Manual on Personal Data (Privacy) Ordinance.

3.18 After reviewing these, the Taskforce believes that the following are opportunities for improving their effectiveness:

Information Security and Privacy Policy

3.19 HA's Information Security Policy and Procedure Manual contains both policy and procedures. Additionally, the Taskforce understands that each cluster can develop its own information security and privacy policy based on the overall HA guidance. There is no single, easy-to-understand information security and privacy policy that is used HA-wide, that is suitable for communicating this message clearly to all HA staff.

3.20 Separating the key policy from other more detailed procedures would also aid communication and make it more accessible.

Strategy

3.21 The importance of maintaining a high level of information security and privacy of patient data needs to be explicitly stated as an objective with clear strategies and measurement of achievement. This *re-acknowledge*ment would help sustain the focus on information security and privacy and build further commitment. The statement of strategies, plans and measurable targets, through the existing annual planning process, at both the corporate and cluster levels, would also enhance communication.

Guidance

3.22 As we have noted earlier, HA has developed a considerable number of information security and privacy standards, guidelines and training materials for its staff. Some are detailed, others more basic and practical. However, the Taskforce believes that they are too generic, aimed at all staff, without providing concrete guidelines for different user groups. They also do not always clearly and simply say what staff should do. What is required by frontline staff most of the time is likely to be more focused, more specific to their job functions. Guidelines that are customised for a specific job function (doctor, nurse, clerical support, researcher and so on) and which point to where more detailed guidance can be found, if required, would better achieve the intended purpose.

3.23 Additionally, simply issuing guidance through the normal channels may not achieve the intended purpose. Requiring this guidance to be periodically discussed in frontline teams, including how it will be applied in their work areas, will further aid both understanding and compliance.

Privacy Impact Assessment (PIA)

3.24 Projects that involve personal information inevitably give rise to privacy concerns. Undertaking a Privacy Impact Assessment (PIA) is a common way of ensuring that that these concerns and safeguards are addressed. The Taskforce is therefore of the view that strengthening existing guidance to require all HA projects that involve personal identifiable information to consider information and privacy throughout the design or re-design of the system would help promote system design choices that comply with the principles established in the PDPO. Full PIA should be required for major projects with HA-wide or community-wide applications.

Retention Policy

3.25 Minimising the length of time that data is held will reduce the risk of loss or unauthorised access. The Taskforce understands that patient data in major clinical systems, such as ePR, needs to be held for lengthy periods to facilitate care delivery. However, the length of time that secondary data, such as data in feeder systems and back-up copies, is held could likely be reduced. Existing retention policies therefore need to be reviewed to ensure that their coverage and timeframes are commensurate with PDPO Data Protection Principle 2 – that personal data is kept no longer than necessary.

External Parties

3.26 Much of HA' s efforts in education and culture building have been directed at its own staff. Third parties, such as IT contractors, honorary appointees, researchers, confidential waste disposal contractors, and so on, may also have access to or handle patient data. Standard contracts with these third parties already include contractual obligations in respect to privacy matters but these could be enhanced by inclusion of obligations to comply with the requirements of the PDPO. Depending on the nature of their role, these third parties may also need to be included/targeted in education programmes, e.g. annual refresher training.

3.27 While contractual terms place obligations on third party contractors, HA also needs to know whether they are complying with these obligations. A planned programme of assurance needs to be established for this purpose. This could be done via Internal Audit or via an independent third party and should be based on assessed risk.

Monitoring and Audit

3.28 HA' s information security arrangements are designed to avoid placing unnecessary restrictions on the delivery of patient care and recognise the need for a balance between security and privacy and operational requirements. Monitoring and audit therefore should play key roles in *detecting* irregularities, ensuring compliance with policy and procedures and in identifying areas for improvement. It also needs to be timely.

3.29 Concepts such as ' Green, Amber and Red Zones' have been developed in the relevant HA manual to help focus and stratify the audit process based on risk. However, the Taskforce understands that these Zones have not yet been fully implemented, and that current audits are based on Green and Non-green Zone parameters. The stipulated requirements and the actual audits need to be aligned.

3.30 The Taskforce also understands that monitoring and auditing is tasked to be carried out at the hospital, cluster and corporate levels and examples presented demonstrate that this can be an effective measure. However, the timing and extent of these audits varies considerably across these areas. This inconsistent and potentially overlapping approach can mean that irregularities and non-compliances may go undetected.

3.31 The importance of this measure warrants HA' s development of a single consolidated programme that is both structured and systematic in design and makes use of available technologies for filtering and focusing this work. This can be based on the substantial good work that has already been done. Approaches such as profiling and data mining should also be adopted to increase the cost-effectiveness of the arrangements.

3.32 The overall audit programme also needs to be led by a single officer who should be responsible for the development of audit strategies, as well as providing tools and specialised training, and receiving reports. This programme will also need to be resourced appropriately.

People

3.33 HA' s patient data users should be highly alert in handling such 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.

3.34 HA has utilised a range of measures to advance such a mindset, including:

- ♦ Promulgating and communicating its policies and guidelines to its staff through various available channels:
  - regular circulars;
  - Cluster IT committees;

  - staff education and awareness raising forums, internal newsletters, videos and practical guides; and
  - clinical IT system features, e.g 'Frequently Asked Questions' (FAQs).

- HA' s Code of Conduct, governing staff' s behaviour, also reminds all staff that:

  "*We have a responsibility to protect HA's and our patients' information, records and property from improper disclosure, misuse or damage.*"

- Upon user account creation application, the staff member applying must sign a patient confidentiality undertaking. Additionally, at each user sign-on, a message is also displayed to remind users to maintain patient data privacy and confidentiality.

- All new frontline staff joining HA receive an orientation that includes elements on information security and privacy according to their job function.

3.35 The Taskforce was provided with a chronology of information security and privacy educational and training programme/workshops that had been conducted over the years. The Taskforce noted that while considerable training had been conducted, particularly in the period immediately after the promulgation of the PDPO in 1996, this did not seem to be part of an ongoing, integrated programme.

3.36 The incidents described in Chapter 2 also indicate that more needs to be done to sustain information security and privacy awareness amongst HA staff at the required high level. Existing information security and privacy education/awareness raising measures need to be redeveloped into a more sustainable and integrated programme that will help ensure staff apply information security policies and principles in their day-to-day roles and behaviours.

3.37 HA has already developed an extensive suite of well regarded e-Learning programmes. Using this accepted technology for an annual refresher course, together with an end-of-unit test, would provide an effective means to deliver such training and ensure a satisfactory level of understanding.

3.38 The Taskforce is also of the view that the visibility of senior management commitment is a key factor in raising the profile of information security and privacy with frontline staff. Incorporating this important theme into regular executive walk-arounds is one way that this can be achieved.

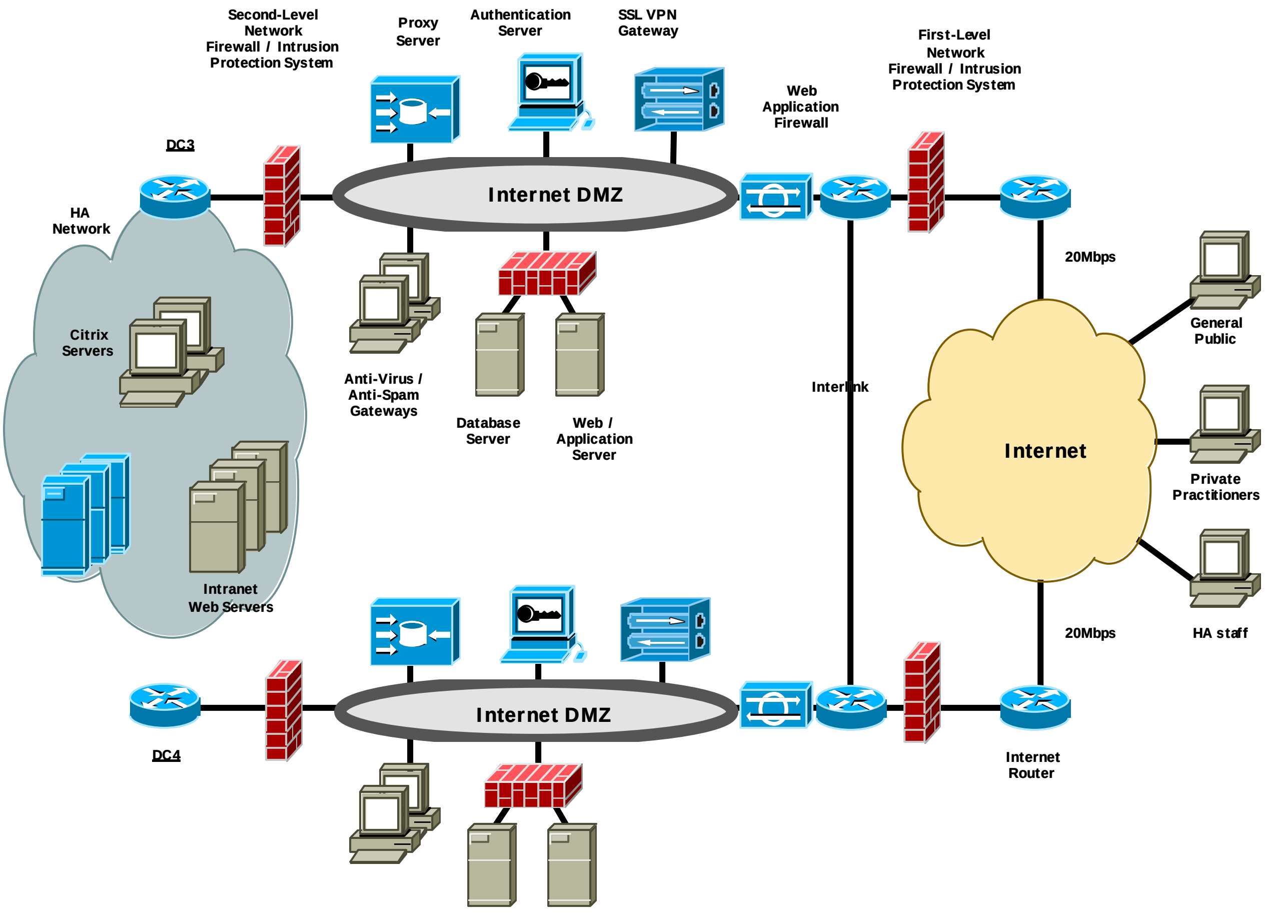
3.39 Clusters also need to know how well their awareness raising efforts are working. Conducting a periodic information security and privacy culture survey, that engages staff and aids two-way communication, is one way to do this. Results can be used to identify which channels are most effective, which staff groups require further attention, and adjustments that need to be made to improve the awareness raising efforts.

Technology

3.40 As well as relying on peoples’ behaviour, the Taskforce considers that greater reliance should be placed on technological solutions for data protection that are, where possible, transparent to the users in order to enforce security.

3.41 Technology-based information security and privacy measures that are already in place include:

- an advanced security infrastructure comprising firewalls, intrusion protection and URL-filtering systems for safeguarding patient data from unauthorised access or malicious attacks, as shown in the following diagram:-



- access to HA’s clinical data systems is controlled through role-based access privileges determined under the established principles of *Patient Under Care*’ and/or ‘*Organisational Need to Know*’. These granted access privileges determine what an authorised staff member can do and cannot do;

- where remote access to clinical data is required, e.g. for supporting consultation at residential care homes, two-factor authentication is employed using security tokens and information is protected over the Internet using SSL VPN;

- HA’ s clinical information systems also keep an audit log for all access transactions by end-users. This audit log includes System User ID, Transaction Date / Time, Workstation ID, Patient HKID & Name that has been accessed, Case No. and transaction that has been made;

- the Clinical Data Analysis and Reporting System (CDARS), the main source for research data, was modified in early 2008 to automatically encrypt all downloaded data from that system. This approach was, however, not extended to other download functions across other systems to mitigate similar risks.

3.42 The following specific technology based opportunities for improvement were noted by the Taskforce in addition to those in Chapter 2.

User Identification and Authentication (I&A)

3.43 HA already uses two-factor authentication for remote access to its clinical data. This addresses the inherently higher risk of attack where an attacker could be anywhere in the world and no physical or procedural controls can be applied.

3.44 The threat environment within different HA facilities and hospitals is different and the approaches to strengthening user I&A should reflect this difference. While the first priority should be to enforce consistent user I&A policies across all systems, alternative forms of user I&A, such as the use of swipe or proximity cards, should also be examined.

3.45 Existing measures to ensure access privileges are reviewed timely on transfer and revoked on exit may also need to be strengthened.

Detecting potential misuse of patient data by HA staff

3.46 The existing deployment of user I&A and access controls within HA clinical systems addresses the issue of restricting access to patient data to those who need it in order to perform their official responsibilities. These technologies cannot, however, control the subsequent use of patient data.

3.47 Given the dynamic nature of clinical environments and the paramount importance of ensuring timely access to patient data in order to provide care, the appropriate technological approach for ensuring proper use of patient data is one of timely monitoring and response to data use and flow. Comprehensive logging and reporting is required.

3.48 Automated tools will be required to assist in processing the large amounts of data that will be stored in the audit log and to help correlate the log data from different applications. Ideally, these tools should be able to identify incidents that require further investigation.

Evaluation of new technologies

3.49 The fast pace of Information & Communications Technology innovation provides the HA with many opportunities for enhancing patient care and operational efficiency. With these opportunities there are also risks if information security and privacy considerations are not incorporated into their adoption.

3.50 The early identification of the potential risks/opportunities arising from new technologies will enable HA to respond in a timely and effective manner.

Chapter 4: Actions and Recommendations

4.1 This chapter summarises the key actions and the Taskforce' s recommendations from our review of both *The Incidents* and *The HA's Personal Data System* under the headings Policy, Structure and People, Procedures and Guidance, and Technology.

4.2 Many of the recommendations are designed to strengthen the leadership and oversight by HAHO and cluster/hospital management; put in place a more systematic, consistent approach to evaluating and ensuring data security and privacy; and build and sustain privacy awareness. Moreover, we have made a significant number of recommendations suggesting the use of technology to further reduce information security and privacy risks, to enforce security measures and to help users in managing data under their care. Some of these technology recommendations have already been actioned or are underway.

Policy

R1 *A single, clearly stated HA-wide Information Security and Privacy Policy should be developed, embedded HA-wide and made readily accessible*.

4.3 HA should have a single Information Security and Privacy policy that is applicable HA-wide. Clusters/hospitals should not develop their own policy as this can introduce inconsistencies. Clusters can continue to have local guidelines but these must be based on the HA-wide policy.

4.4 The policy document drawn up by the Taskforce at Attachment 5 is designed to clearly state:

- the importance to HA of maintaining the confidentiality, integrity and availability of personal information and HA' s commitment to preserving the security and privacy of personal information it holds;
- all identifiable personal information is to be accorded the highest level of security and privacy protection;
- this protection should be in accordance with the requirements of the PDPO;
- all HA employees, and non-HA employees who are involved in the handling and processing of patient data, must comply with this policy;
- staff are encouraged to report possible security and privacy breaches; and
- persons responsible for such deliberate violations and breaches may be subject to disciplinary and legal actions.

4.5 This policy document is recommended by the Taskforce for HA' s consideration. Once approved, the policy document needs to be made readily accessible and become a key part of all relevant education and training programmes, and upon which guidelines and procedures should be based.

R2 *The role and strategic importance of information security and privacy should be clearly articulated and subsequently reinforced through the existing annual planning process at both corporate and cluster levels.*

4.6 As we noted in our earlier findings, the importance of *information security and privacy* has been well recognised by HA since its inception and was the focus of significant efforts at the time of enactment of the PDPO. However, our review suggests that this programme would benefit from:

- a re-acknowledgement of this importance;
- a holistic statement of strategy that articulates its goals and how these will be achieved, including the approach for ensuring compliance; and
- a clear statement of priority that can be collectively used to drive HA's information security and privacy programme as part of Enterprise-wide Risk Management.

4.7 Important major information projects, such as the new generation of CMS and eHR, would also likely benefit from making information security and privacy a visible priority through the existing annual planning process. This explicit priority also needs to be cascaded to the cluster/hospital levels, and be translated into meaningful and measurable targets.

Structure and People

R3 *To further enhance leadership and governance of information security and privacy, HA should:*

- ♦ *appoint a Chief Information Security and Privacy Officer (CISPO) who should report to a senior level and should lead the HA-wide Information Security and Privacy programme, and be responsible for driving forward improvements in a co-ordinated, integrated manner;*
- ♦ *establish a HAHO committee that has specific responsibility to oversight all HA-wide information security and privacy matters;*
- ♦ *revisit relevant cluster/hospital committee structures to ensure a clear role and a specific focus on information security and privacy with appropriate linkages; and*
- ♦ *further define, formally document and communicate the role and responsibilities of Data Controllers across HA. This should include explicit responsibility for the people-related aspects of information security and privacy such as education and training.*

4.8 Again as we noted earlier, under opportunities for improvement, HA's information security and privacy programme needs to be made more sustainable by the appointment of a dedicated CISPO who has deep professional expertise and whose responsibility is to lead, coordinate and monitor the programme. One of the appointee's first tasks will be to establish an appropriately skilled team to support him. Success will also require a member of HA' s senior executive management team, to whom the CISPO should report, taking up the active sponsorship of the programme.

4.9 Establishing a HAHO committee to oversight information security and privacy should ensure an enhanced focus on this important subject. To be effective this committee would need to have effective linkages with other relevant committees, especially with those at the cluster level. This could be achieved through elements of cross-committee membership and reporting lines.

4.10 Further defining the role and responsibilities of Data Controllers across HA could enable these important posts to more effectively carry out their duties. Including responsibility for the people-related aspects should facilitate hospital-wide education and training that includes a greater focus on the principles established in the PDPO.

R4 *Cluster Chief Executives (CCEs) should have an explicit accountability for information security and privacy within their cluster and should be required to make an Annual Information Security and Privacy Report to HAHO that includes:*

- *results of cluster-wide Information Security and Privacy risk assessment;*
- *continuous improvement measures taken; and*
- *Key Performance Indicators (KPIs) that demonstrate the effectiveness of their overall information security and privacy programme within the cluster.*

4.11 In HA' s decentralised management structure, CCEs are accountable to the HA Chief Executive for the operations of their respective clusters. Including *information security and privacy* as an explicit accountability of the CCE, measured and reported annually using designated KPIs, would be a necessary ingredient for success.

R5 *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, and would include:*

- *an information security and privacy workshops for staff covering a common component on overall policy and general data protection principles as per the PDPO, plus a tailored component targeting specific functional areas for the specific staff groups;*
- *an induction pack for new staff that includes greater emphasis and training on information security and privacy elements;*
- *an information security and privacy e-Learning refresher training module applicable to specific staff groups that reminds and updates staff about the risks and of their responsibilities and the professional duty of care, and includes a test, to be completed annually by all staff; and*
- *regular and planned use of all available channels to keep up staff awareness on information security and privacy.*

4.12 Technological measures are important but on their own are not sufficient to ensure a fully successful information security and privacy programme. They must be complemented by people measures. It is important therefore that HA ensure that its staff, at all levels, understand their responsibilities for information security and privacy and apply HA's policies and principles in their day-to-day roles and behaviours.

4.13 Since the incidents, and with the immediate measures already implemented, staff undoubtedly have a greater awareness of the importance of information security and privacy. However, in an organisation the size and complexity of HA, an ongoing, well planned and integrated programme is required. This should include tailored, face-to-face training targeting specific functional areas for specific staff groups, as well as a common component centred around HA's policy and the data protection principles as set out in the PDPO.

4.14 HA's e-Learning platform would provide a valuable, established method for annual refresher training. Again tailoring specific elements to a staff member's job would increase its effectiveness while requiring satisfactory performance in an end-of-module test would help to ensure the messages are understood. Human Resources training staff would likely provide a valuable resource in the overall design and delivery of these education/training programmes. A system of Privacy Ambassadors at the frontline level could also be considered.

R6 *Increase the visibility of senior management in relation to information security and privacy by, for example, incorporating it as a prime element in regular executive walk-arounds. Each cluster could also undertake a periodic information security and privacy culture survey to help monitor the effectiveness of their awareness raising programme and to identify areas for further improvement.*

4.15 Visible support from the top is always important. Including information security and privacy in regular executive walk-arounds will help send, reinforce and sustain the message to the frontline. This will also provide useful, direct feedback to top management on the success of their awareness raising programme, as well as identifying areas for improvement.

4.16 Results from an information security and privacy culture survey, using a centrally designed survey instrument, would provide valuable feedback, allowing trending and cross-cluster comparisons to be made and could be used as a Key Performance Indicator (KPI).

4.17 Importantly, these processes should also help strengthen two-way communication.

Procedures and Guidelines

R7 *Existing information security and privacy procedures and guidelines should be:*

- *redeveloped for different user groups, such as doctors, nurses, clerical staff, researchers, in simplified, easy to understand and more accessible form, that states in concrete terms what they should and should not do while pointing to where more detailed guidance can be found; and*
- *required to be regularly discussed in frontline teams - both its contents and how it will be applied in their work area.*

4.18 As noted earlier, HA has published a significant number of information security and privacy policies, standards, guidelines and training materials that cover a wide range of topics. The Taskforce believes that guidelines that are customised for a specific job function (doctor, nurse, clerical support, researcher and so on) while also pointing to where more detailed guidance can be found, would better serve the needs of frontline staff.

4.19 The current body of HA security materials can be drawn on and built upon to create actionable guidelines that cover all the important points in simplified, easy to understand and more accessible form that make it easy for staff to know what they need to do in order to protect patient data. The current more detailed guidance could then be retained for those that need it. Periodically discussing these guidelines in frontline teams, and how it will be applied in their work areas, would further aid understanding and influence behaviour.

4.20 An initial exemplary security guideline should be developed to be used as a model for the others. This would include guidance directly relating to the handling of patient data, both electronically and manually, as well as general best practices, e.g. strong password selection, that pertain to their work.

R8 *Strengthen guidance 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.*

4.21 Requiring all projects that involve personal identifiable data to explicitly take account of the information/privacy policy and the principles established in the PDPO will ensure they are considered. The level of assessment required will depend on the sensitivity of the data and full PIAs should be required for major projects with HA-wide or community-wide applications.

4.22 The performance of PIAs should be closely linked with the Secure Information Workflow Reviews of R24 to ensure that sufficient technological protections are applied to ensure the privacy of patient data. A record should be kept of the technologies selected to address specific privacy concerns so that the HA can build a repository of solutions. This body of knowledge can help expedite the development of applications in the future

R9 *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. Measures to make sure access privileges are reviewed on transfer and revoked on exit in a timely manner should also be enforced.*

4.23 Under HA' s decentralised management environment, these two directives are utilised by clusters/hospitals, along with role-based standard templates, for determining the access privileges of their staff. Provision of additional guidance would help to further ensure consistency across clusters. Ensuring allocated access privileges are kept up-to-date when staff change jobs or leave the hospital is also essential.

R10 *Implement a mandatory three-step test before download privilege is approved to minimise downloading of patient identifiable data:*

- ♦ *Can this function be ceased or performed in another way?*
- ♦ *If no, can we modify the workflow in practical terms so downloading is not required?*
- ♦ *If no, can patient identifiers be removed or pseudo identifiers used?*

This three-step test should also be retrospectively applied to all existing approvals and at least every 12 months thereafter.

4.24 This three-step test is designed to minimise downloading of identifiable patient data from HA' s clinical systems to only those times when it is absolutely necessary and should apply to both new requests and retrospectively to existing approvals.

R11 *To reduce the potential for information security and privacy breaches, HA should renew its retention policy to ensure that personal data is not retained any longer than necessary, as required by PDPO Principle 2.*

4.25 The longer patient identifiable data is held, the greater the risk of loss or unauthorised disclosure. HA' s retention policy should be reviewed and extended to include the holding of electronic data outside the main clinical systems, such as back-up copies, manually collected data, and medical equipment.

R12 *Continue to encourage all staff to report incidents of unauthorised disclosure or loss of patient data in a timely manner through formal adoption of a just culture that differentiates between accidental loss and deliberate unauthorised access.*

4.26 Incident reporting provides valuable feedback and opportunities to learn. If the response is not appropriate to the circumstances, it could reduce the likelihood that staff will report such incidents. The formal adoption of a just culture that differentiates between accidental loss and deliberate unauthorised access, for example, would be more appropriate.

R13 *Rebuild and resource existing monitoring and audit arrangements into a consolidated programme led by the CISPO that is structured, systematic and aligned to detect irregularities and monitor compliance with the PDPO and HA's policies and procedures, and includes:*

- ♦ *clear roles and responsibilities for devising audit strategies, conducting audits and providing HA-wide audit tools;*
- ♦ *reporting of results and taking corrective actions to improve measures as necessary; and*
- ♦ *continuous oversight, adjustment and improvement of the audit strategy to increase its cost-effectiveness.*

4.27 Monitoring and audit are key detective/corrective controls within HA' s data-handling systems. Rebuilding the current arrangements into an appropriately resourced, consolidated programme where roles and responsibilities are clearly defined, strategies established and audit tools provided, would significantly increase its cost-effectiveness. Further development of monitoring tools that are able to better detect irregularities would also enhance current data protection safeguards.

R14 *HAHO should further strengthen 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 by ensuring the requirements of the PDPO are clearly incorporated. A template for such agreements and contracts should be developed for common adoption. Also a planned programme of third party assurance in respect of these information security and privacy requirements should be initiated.*

4.28 Strengthening existing contractual obligations with respect of information security and privacy of third parties, who access or handle patient data, to include requirements of the PDPO would provide greater assurance. These obligations should address the issue of how to securely transfer information between third parties and HA and how third parties protect the information when it is under their control. While the specific measures taken by third parties may differ from those adopted by the HA, the level of protection should be the same.

4.29 HA also needs to have greater knowledge of and oversight over these third parties regarding their compliance with these contractual obligations. This can be reviewed through a programme of assurance via Internal Audit or an independent third party, as appropriate.

Technology

R15 *All corporate IT systems should be urgently enhanced to automatically encrypt and password-protect downloaded identifiable patient data.*

R16 *Introduce, with immediate effect, the mandatory use of advanced USB Flash Drives with encryption and password 'lockdown' for protecting patient data.*

R17 *Upgrade the Advanced Incident Reporting System (AIRS) to better collect, highlight and report data loss incidents.*

4.30 The above three technology recommendations, proposed by HA management to quickly address several issues identified from the reported data loss incidents, are endorsed by the Taskforce and have already been fully actioned.

R18 *HAHO should evaluate the operational requirements for the downloading of patient data from clinical systems and develop technological solutions to minimise this practice as much as possible. Where downloading is required, cost-effective protection technologies that are transparent to the users and commensurate with sensitivity of the data should be deployed.*

4.31 HA has 24 clinical subsystems which have a total of 57 functions that facilitate data downloading. Examining the common reasons for downloading, following completion of the retrospective review of existing approvals by dusters as noted above, may enable further measures such as alternate workflows or technological solutions to be put in place to minimise the downloading of identifiable patient data.

4.32 In those circumstances in which patient identifying information does not have to be included, applications can be updated so that identifying information, such as HKID or name, are not included in the downloaded data.

4.33 In those circumstances, such as research, in which it is necessary to associate multiple medical records belonging to a patient, but knowledge of the patient's identity is not required, an anonymous identifier should be used. The calculation of a message digest or hash function, such as SHA-1 or MD5, on the CMS-internal patient identifier could be used, as this kind of anonymous identifier would make it computationally infeasible to derive the original identifier from the message digest value.

4.34 For those cases in which it is necessary to download patient data with identifying information, the circumstances of its subsequent use, storage, and transmission should be considered when determining what additional protection mechanisms are needed. As part of the effort to minimise the risks facing patient data, the printing of downloaded reports should be minimised. In many cases, the sharing of reports electronically, utilising the protection strategies and technologies outlined further in this section, can eliminate the need for printing and the associated responsibilities for securely handling the hard copy, including its proper destruction. The use of encryption and shared file servers, as described in the requirements below, will play key roles in protecting downloaded patient data.

4.35 Encryption addresses the risks to patient data from external parties who may gain access to the devices on which the data is stored or the networks over which the data is transmitted. An additional potential risk that should be addressed is the unauthorised sharing of patient data after it has been retrieved or downloaded. The types of products that address these types of risks are often referred to as *information or document rights management* or *data leakage protection*. The deployment of these solutions requires more analysis than is needed for encryption because distinctions have to be made between different categories of data and different types of users. The development of an effective information rights management policy, especially in an environment as complex as the HA, requires significant attention.

R19 *Transparent, whole disk encryption should be deployed on portable computing devices, such as laptop computers and PDAs, and on other computers at risk from theft.*

4.36 While increased user training, awareness and enhanced physical protection can minimise the loss or theft of portable computing devices, the risk cannot be eliminated completely. To address this risk, whole disk encryption should be deployed on laptops and PDAs. Encrypting a device' s whole disk ensures that any temporary or deleted files are also protected and does not require HA staff to make decisions about what files should be encrypted or not. They are all encrypted.

4.37 Management of the encryption key used in whole disk encryption can be integrated with the operating system (e.g. Windows) logon so the encryption process is completely transparent to the end user and therefore does not impose any additional security responsibility. To ensure that the HA has continuous access to information on portable devices even if the users are unavailable, there should be a key recovery capability in place. The key recovery feature found in many commercially available encryption products which requires two or more staff to access the recovery key should be used.

R20 *The use of centrally managed file servers as opposed to individual computers should be encouraged for storing patient data.*

4.38 Encouraging the use of centrally managed, shared file servers instead of individual staff' s PCs has several security and operational benefits. First, such file storage eliminates the operational need to copy data to USB Flash Drives and other portable storage devices. Staff can share information in place on a server. Second, it is easier to create a safe environment for information on a server than it is on staff PCs. Third, back up and recovery of data are easier and more reliable on a server than on staff PCs.

4.39 The administration for each file server should be well-defined. This includes having a clear definition of the types of data that will be stored on the server and having a process in place for requesting and approving access to the folders or directories on a server. Proper administration also includes the periodic review of access control rights to ensure that granted permissions are in keeping with the '*patient under care'* and '*organisational need to know*' principles.

4.40 Currently desktop virtualisation technology is being utilised for remote access to HA systems and for some access to CMS. When using this technology, a user does not have access to his local computer's disk and so cannot download any information to it. This would minimise opportunities for the disclosure of patient data and so further use of this technology should be explored.

R21 *Deploy 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.*

4.41 While the use of USB Flash Drives and other portable memory devices can be reduced, there will remain situations in which it is operationally required to use them. To accommodate these situations, technology will be deployed that enforces strict controls over the individual devices that can be connected to HA computers.

4.42 The first control is preventing any non-HA approved device from connecting to a HA computer with patient data. The second control is scanning the contents of approved devices to make sure that viruses or other malware cannot be introduced into the HA from the files stored on one of these devices.

4.43 The third control is to encrypt all of the information stored on them so that even were these devices to be lost or stolen, the risk of data disclosure would be minimised. This encryption, and the management of the associated encryption keys, can be deployed in a way that is transparent to end-users and so the protection of patient data on these devices does not impose any additional user responsibility.

4.44 This technology requires the installation of software on all HA computers that support the downloading of data onto removable storage devices. Patient data downloaded from one HA computer can then only be decrypted when uploaded on to another HA computer. If the device were to be lost or stolen, the patient data could not be accessed nor deciphered by a non-HA computer.

4.45 Another circumstance in which patient data, as well as other sensitive data, is written to portable memory devices is back-up. In these cases, the data may be written to tape, disk, floppy, or USB Flash Drive. The same principle of transparent encryption should apply here, as well. Many commercially available back-up products have encryption features, though not all products have these features enabled by default, and so deployment should ensure that the features are used properly. The use of two-person control should be examined for decryption of back-ups while the use of encryption does not eliminate the need to physically protect back-up media. To ensure that the HA has ongoing access to important data, IT should pay particular attention to the management of encryption keys (passwords) and should periodically test the decryption/recovery process.

4.46 Email can be an effective and secure alternative to the use of portable memory devices for the transport of patient data. However, most email systems in their default configurations do not provide adequate protection. The first step is to enhance the security of HA internal email. This can be done through the configuration of encryption options within Exchange. This may require the centralised management of Exchange servers within the HA.

4.47 Protecting email involves two related, but distinct, tasks. The first is protecting the username and password that are sent from the email client, e.g. Outlook, to the Exchange server. This protects against the risk of an attacker taking control over an email account. The second task is the protection of the email content. For HA-internal email that is processed by HA-managed Exchange servers, both security tasks can be addressed through the same Exchange server encryption configuration, though separate configuration is needed for each type of email client, including web access to email.

4.48 Additional technological solutions are required for encrypting email that is sent to or received from external parties. The protection of email content in these circumstances can be addressed by technologies such as S/MIME. All major email clients include native support for S/MIME and after initial configuration its use is as easy as setting the priority of an email message. Ensuring that the login credentials of external parties are protected is beyond the immediate control of the HA, but the HA can alert these parties to the risk and offer suggestions for remediation.

R22 *Computers containing patient data should be under the administration control of IT Departments and not the control of the computers' users.*

4.49 The protection of patient data residing on end user computers, such as PCs, notebooks, and PDAs requires continuous management that is only possible if these computers are under the control and management of IT. This management covers a broad spectrum of issues, including up-to-date anti-virus and anti-malware, timely application of security patches, personal firewall configuration, and enforcement of policies relating to user authentication and the sharing of files within directories. For example, there should be a policy that prohibits the global sharing of directories. To help accomplish this, all networked computers should be registered in Active Directory and subject to Group Policy Objects.

4.50 Further, it is necessary that the system administrative rights of all computing devices in HA be owned by the IT departments instead of end-users. The creation of a safe environment for patient data requires the deployment of additional security technologies on HA computing devices. Examples include the endpoint security and encryption solutions referenced in these recommendations. In order for the ongoing protection of patient data to be ensured, it is necessary that these additional technologies cannot be disabled or bypassed. It is also necessary to prevent the additional installation of software, such as that used in P2P networks, that could lead to the unauthorised disclosure of patient data. These requirements dictate that users do not have any system administrative privileges on their computers.

4.51 IT department administrative control should extend to medical systems, such as PACS and PMS. In addition to addressing the previous requirements as appropriate, attention should be paid to the risks arising from network connectivity, in particular external vendor connectivity.

R23 *Comprehensive logging and reporting should be deployed to assist in detecting possible misuse of patient data by HA staff, IT administrators and external parties.*

4.52 The first step in accomplishing this is through reconfirming the set of relevant user and system activities that should be logged. This will involve events that can be logged by the *Commercial Off the Shelf* (COTS) products used within the HA as well as events that are logged by HA-developed applications. It may be the case that HA-developed applications will have to be enhanced to log additional events and that specialised logging and auditing tools will have to be deployed. To support accountability, all administrators should use named accounts and not default administrative accounts and there should be no sharing of accounts unless other, strong procedural measures are in place to identify who is using a particular account at a particular time. The logging should cover vendor access, both from within HA as well as remotely.

4.53 The computing infrastructure to support logging and reporting will need to meet the following requirements. The log records need to be maintained in secure storage so that individual records cannot be modified or deleted and so any patient data contained in the records is protected. The storage needs to be sufficiently large that records can be kept as long as is necessary for both initial and follow-on analysis. Automated tools will be required to assist in processing the large amounts of log data that will be created and to help correlate the log data from different applications. Ideally, these tools should be able to identify incidents that require further investigation.

4.54 The review of log data should be carried out by individuals well versed in HA operations and who are not themselves subjects of the logging that they are reviewing. They should have clear guidance on identifying events that need further review and there should be a well-defined escalation process.

R24 *Perform Secure Information Workflow Reviews in accordance with the Four Principles for Enhancing Patient Data Protection.*

4.55 The selection and deployment of technological security measures should be informed by the operational requirements and environments in which patient data is used. The Secure Information Workflow Reviews can identify how changes in software application functionality and user operating procedures can improve patient data protection as well as help develop specific requirements for additional security technologies.

4.56 An important element of these reviews is evaluating the appropriateness of security technology in light of the operational (and system) environments, which may include private doctors and hospitals, in which patient data is accessed and stored. In these higher risk environments, additional protections, such as the selective encryption of personally identifiable information, may be called for.

4.57 The performance of these reviews should be carried out under the auspices of the CISPO to provide consistency across the HA and to leverage staff expertise. The performance of these reviews will involve cluster/hospital system users, administrators, and developers and so becomes another avenue by which information security knowledge and best practice can be promulgated throughout the HA. Budget will have to be provided to fund the application changes that are indicated by the reviews of existing systems and the performance of these reviews should be incorporated into the overall process for the development of new applications.

R25 *Technologies should be deployed and associated procedural guidelines promulgated to proactively strengthen user Identification and Authentication (I&A) in support of controlling access to patient data and holding users accountable for its use. Measures should be commensurate with the threat environment.*

4.58 As noted earlier, HA already uses two-factor authentication for remote access to its clinical data and other support functions. The threat environment within different HA facilities and hospitals varies and the approaches to strengthening user I&A should reflect these differences.

4.59 The first priority should be to enforce consistent user I&A policies across all systems. The policy areas that should be addressed include minimum password length, password composition, password history, password renewal and response to repeated failed login attempts. The goal is to promote the selection of passwords that are easy to remember and difficult to guess.

4.60 There should be notices and warning messages to alert users to potential situations in which their login credentials, viz. username and password, may have been compromised. These include notice, at the time of logon, of the date and time of the last successful logon, as well as any previous failed logon attempts. There should be a warning notice whenever a user logs on to a system multiple times and the recommendation to close any unused sessions.

4.61 The protection of passwords within the IT systems should be enhanced so that passwords are always encrypted when being transmitted over networks and that they are stored as salted message digests (hash values). These measures will prevent administrators from being able to impersonate users.

4.62 To enhance productivity and convenience in clinical environments, alternative forms of user I&A, such as the use of swipe or proximity cards, should be examined.

R26 *The CISPO, supported by HA IT Services, should be made aware of new technologies that are being considered for HA use and should keep pace with the introduction of new information security technologies and strategies.*

4.63 The CISPO, supported by HA IT Services, should evaluate new technologies under consideration to ensure that they can be adopted in a way that ensures the ongoing protection of patient data. The use of USB Flash Drives is one example of a technology that would have come under CISPO review had the position already been established. Identifying early the potential risks/opportunities will enable HA to respond in a timely manner.

GLOSSARY OF ABBREVIATIONS AND KEY TERMS

AIRS — *Advanced Incident Reporting System – a reporting system serving as a tool to support risk management by facilitating the reporting, classification, analysis and management of incidents.*

Amber Zone — *This is the medium security risk level devised by HA. It represents where access to patients' data is not covered by the Green or the Red Zones.*

Brute Force Attack — *A method of defeating a cryptographic scheme by trying a large number of possibilities*

CDARS — *Clinical Data Analysis and Reporting System – a retrospective decision support system which provides value-added clinical information to support clinical audit, data analysis, reporting and research in the HA.*

CMS — *Clinical Management System – an electronic system adopted by the HA to process information, including patients' data, for the provision of medical services.*

COTS — *Commercial-Off-The-Shelf. It refers to a technology or computer system that is ready-made and available for sale, lease, or license to the general public.*

Data Controller — *The person(s) nominated by each hospital with the function to ensure compliance with the PDPO.*

Data Protection Principle — *The data protection principles in Schedule 1 of the PDPO.*

Data Mining — *Process of analyzing data from different perspectives and summarizing it into useful information*

DSS — *Decision Support Systems*

Encryption — *The process of scrambling files or programs, changing one character string to another through an algorithm (such as RC4). Encryption is a way to disguise information so that it cannot be read easily, except by the intended recipient with the key.*

eHR — *Electronic Health Record. An information system for healthcare professionals in both public and private sectors to enter, store and retrieve patients' medical records, subject to authorization by the patients.*

ePR *Electronic Patient Record. A system provides patient-centred life-long longitudinal medical records for medical history references.*

Green Zone *This is the low security risk level devised by HA. It represents where access to patients' data is supported by patient attendance / admission at that hospital or is within a short period time after that.*

HAHO *Hospital Authority Head Office.*

HKID *Hong Kong Identification Card Number*

Identification and Authentication *Identification is referred to recognizing users on a system by using unique name, and authentication is the process of determining whether someone or something is who or what it is declared to be.*

KPIs *Key Performance Indicators – KPIs are financial and non-financial metrics used to help an organisation define and measure progress toward organizational goals.*

LIS *Laboratory Information System*

Malware *Also known as Malicious Software, is software designed to infiltrate or damage a computer system without the owner's informed consent.*

Non-Green Zone *This is where access to patients' data falls outside the ambit of Green Zone.*

Organizational Need to Know *A principle formulated by the HA for controlling access to patients' data held by it. Under the "Organizational Need to Know" Principle, access to patients' data is allowed for various necessary purposes other than the purpose of Patient under Care.*

Patient under Care *A principle formulated by the HA for controlling access to patient data held by them. Under the "Patient under Care" Principle, health care professionals who are involved in the care of a patient have the right of access to clinical data which is relevant to that care.*

PDA *A Personal Digital Assistant is a handheld computer.*

PDPO

Personal Data (Privacy) Ordinance. The Ordinance has come into effect on 20 December 1996 in Hong Kong. It regulates the collection, storage, protection and use of data related to living individual from which it is reasonably practicable to identify the individuals.

Personal Data

Section 2(1) of the PDPO defines "personal data" to mean 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.

Personal Data System

Section 2(1) of the PDPO defines "personal data system" to mean any system, whether or not automated, which is used whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system.

PII

Personally Identifiable Information

Red Zone

This is the high security risk level devised by HA. It represents where access to patients' data carries a high security risk, e.g. access to hospital employees' clinical data or access to data of patients of public interest.

Security Tokens

Physical device that an authorized user of computer services is given to aid in authentication

USB Flash Drive

A flash memory data storage device integrated with a USB (Universal Serial Bus) connector.

Attachment 1

Table 1: Summary of ten reported electronic data loss incidents involving identifiable patient data over a period of some 13 months to 5th May 2008

#	Date	Location	# of Patients	Down-lo aded	Electronic Device	Protected	Type of Data Involved
1	12-Apr-07	PYNEH	43	No	USB Flash Drive	No	Name, phone no.
2	20-Jul-07	PYNEH	3	No	Digital Camera	No	Name, HKID no., hospital number, DOB, clinical of patients' wound
3	19-Sep-07	TMH	1755	No	Laptop Computer	Yes	Name, age, gender, hospital no., date of admission and discharge, clinical physical score
4	17-Oct-07	KH	13	Yes	Palm Handheld	Yes	Name, HKID no., gender, age, diagnosis, nursing therapeutics required
5	20-Oct-07	UCH	26	No	USB Flash Drive	No	Name, HKID no., DOB, marital status, surname of spouse, date of current delivery, phone no. and address
6	28-Oct-07	SYP	3000	No	Desktop	Yes	12 patients: Chinese name, telephone no. address
					Removable Disk		3000 patients: research data, no personal data
7	14-Nov-07	PYNEH	743	No	USB Flash Drive	No	HKID no., gender, age on admission, clinical photos and clinical information of one patient
8	March-08	KH	31	No	MP3	No	Name, HKID no., nursing discharge summary, incident reports
9	15-Mar-08	PYNEH	150	No	USB Flash Drive	Yes – 129 No – 61	Name, DOB, Age, date of admission, reason of admission, diagnosis, medication, dosage, progress, case doctor and nurse, consulting team and date of home leave
10	1-May-08	PWH	10000	Yes	USB Flash Drive	No	HKID, name, lab test title, request location & unit, test request date, authorization date, unit price

Notes: Downloaded = Yes, means the data was extracted electronically from an IT System

Downloaded = No, means the data was created manually from paper based records such as Physical Medical Record, other Documents or even Printouts

Technological Strategies for Protecting Patient Data

The selection of security technologies should:

- be made in the context of the complete lifecycle of the information that needs protection,
- directly address recognized risks,
- have minimal impact on end-users.

Addressing the data loss incidents

All of the incidents involved the loss of portable devices containing patient data. The two most straightforward approaches to addressing this risk are to either stop storing patient data on portable devices or encrypt the data so that it cannot be disclosed even if the device is lost or stolen.

Eliminate need for removable media

Modify Workflow

In the PWH example, it was shown that by installing the necessary software on a clerical staff' s computer the need to copy data onto a USB drive was eliminated. This solution is very specific to the PWH case, but is an example of an approach that can be applied elsewhere.

File Server

One of the other general reasons for copying data onto removable media, such as USB drives, is for sharing the data with colleagues. This can be accomplished through the alternate use of a file server with shared folders. For this to be effective it is necessary that someone is responsible for determining and setting access control permissions for the content on the file server and that any remote network access to the file server is protected. This is a straightforward solution that can eliminate many of the situations in which removable media is currently being used and so directly addresses the risks in many of the incidents. This approach cannot, by itself, prevent users from copying data to removable media if they want to and so does not protect against that threat.

Encrypt data on portable devices and removable media

While encryption is a powerful technology, its effectiveness can be diminished because encryption keys are difficult to manage. The availability of encryption options vary according to the device in question.

- ***Laptop computers***: Patient data on laptop computers should be protected by whole disk encryption, and not through the encryption of selected files or directories. File or directory encryption does not protect temporary copies of files made automatically for recovery purposes, nor, depending on implementation, deleted files. And it may be the case that patient data exists in files that are not stored in the encrypted directories. Also, with whole disk encryption, access can be linked to the Windows logon so there is no impact on the user, as opposed to file or directory encryption in which cases the user needs to remember an additional password. Also, many whole disk encryption products include a corporate key recovery function so that access to data is possible even if the laptop' s user is not available. If physical control over desktop computers cannot be guaranteed, as was the case at SYP, then whole disk encryption should be considered for them, as well. Example product: GuardianEdge Hard Disk Encryption

- ***PDAs***: The considerations for encryption on PDAs are the same as for laptop computers. The products that protect PDAs also protect smart phones. The example product is available on the devices used in community nursing. Example product: GuardianEdge Smartphone Protection

- **Digital cameras**: Encryption for digital cameras is not widely available and is generally targeted to professional photographers concerned about intellectual property protection. An alternative approach is to use the camera in a smart phone and rely on the available encryption (see above).

- ***USB memory sticks, MP3 and other removable media***: If the use of removable media cannot be eliminated, there are several options. The easiest to deploy is a USB with built-in encryption, such as Kingston' s Data Traveler Vault Privacy, which has been deployed by the HA. This does address the specific risk of a lost device or a device that was stolen without the specific intent of accessing patient data. But there are several drawbacks. These include the inconvenience that a user has to enter password and copying files takes longer because of launching the application, and the use of the devices is not enforced by the system. Since a common password is used, this would not provide protection from someone specifically targeting the HA. From a security functionality perspective, the baseline requirement is the ability to encrypt patient data as it is being moved from one HA computer to another via removable media, without imposing new responsibilities on the user. Additionally, it is desirable to be able to control what devices can connect to HA systems, ensure that HA systems are protected from any malware that may be introduced from files on these devices, and be able to log the movement of files on these devices. Example product: Check Point Endpoint Security Media Encryption

Types of unauthorised disclosure of patient data and response

Unauthorised disclosure of patient data can be the result of either deliberate or accidental action. In all of the reported incidents, there was no deliberate effort on the part of the involved parties to compromise patient information. In all cases, the involved parties were undertaking legitimate activities that involved access to patient information. The potential disclosure of patient data in these cases was due to the loss or theft of the computing, digital, or storage device on which the patient data was stored. Given these circumstances, the appropriate remediation approach is to modify workflow, apply protection technologies, and provide security and privacy guidance in such a way as to provide a safe environment in which they can perform their duties. The Four Principles for Enhancing Patient Data Protection provide direction on creating this safe environment.

In addition to accidental disclosure, the privacy of patient data is also at risk from unauthorised access that doesn't comply with the "patient under care" and "need to know" principles. Examples include HA staff who view medical information about colleagues, relatives, and other people of interest, either for their own purposes or on behalf of some third party. In contrast to the case of accidental disclosure where the protection of stored data at rest is paramount, deliberate unauthorised access takes place through the use of HA IT applications and systems. Further, these kinds of unauthorised access take place without the individuals in question bypassing any of the IT protection mechanisms. In other words, the access controls within applications such as the CMS or LIS have been set to allow them access.

Given that the primary reason for maintaining patient data is to support medical care and that the dynamic nature of a clinical environment makes it impossible to determine a priori each of the individuals who might need access to a patient's information in order to deliver care, there are inherent limitations in addressing this type of unauthorised access purely through access control mechanisms such as roles. Timely and targeted monitoring of user access to patient data is the more appropriate, though more challenging, approach.

The process of monitoring starts with an iteration of the types of unauthorised access and the characteristics that can be captured through application-based monitoring or logging. This could include off-hours access to patient data, access to HA staff data, access to data on notable individuals, or access to data on patients not currently under care. The second step is to process and present this information in a way that is easy to review. This is not an easy task given the high level of use of HA systems. The third step is to have staff formally assigned the task of reviewing these logs and following up on suspected violations. For both technological and compliance reasons it is not possible to log all types of unauthorised access, such as to a relative's data. To address this limitation, there should be additional random review of patient data access.

In addition to addressing the issue of preventing unauthorised disclosure of patient data, it is necessary to address the response, including any disciplinary measures, to a disclosure. The two types of unauthorised disclosure are very different in circumstance and motivation and the responses should differ accordingly. The accidental loss of sensitive information, such as patient data, is a reality of today’ s world and is often due to systemic problems and not just the actions of the individuals directly involved. Achieving the goal of greater patient data protection is not served by punishing staff involved in this type of incident and could have the negative effect of discouraging the reporting of such incidents, thus exacerbating the problem. Deliberate unauthorised access to patient data, on the other hand, is a direct violation of trust and should be punished accordingly. The actions taken should serve not only as punishment for the individual involved in an incident, but also as a warning to others that this type of activity won’ t be tolerated.

Secure Information Workflow Methodology

The Secure Information Workflow Methodology provides a consistent way of applying the Four Principles for Enhancing Patient Data Protection across HA operations in a way that leverages security knowledge within the HA and minimizes impact on end-users. It is based on the methodology introduced in the Harvard Business School Press Book *Digital Defense: What You Should Know About Protecting Your Company's Assets* and shifts the burden of protecting patient information from end-users to system designers. It does this by an analysis process that provides clear direction on how to create safe environments for patient data in which the security responsibilities of end-users are minimized. This direction may include changes to existing HA applications, introduction of new technical or physical protections, or changes in operating procedures.

The methodology was applied to the Pathology Department at PWH where one of the incidents took place and identified how a change in the way in which an application grouped exported laboratory test information could not only eliminate the operational need that led to the copying patient information onto a USB device, but also reduce clerical staff workload.

The methodology (pictured below) begins with an information gathering phase that documents the flow and processing of patient data within the activity under review. This starts with identifying the external sources of patient data involved in the activity. These could be hard copy forms, faxes, audio tapes, email or files downloaded from CMS or a cluster or hospital system.

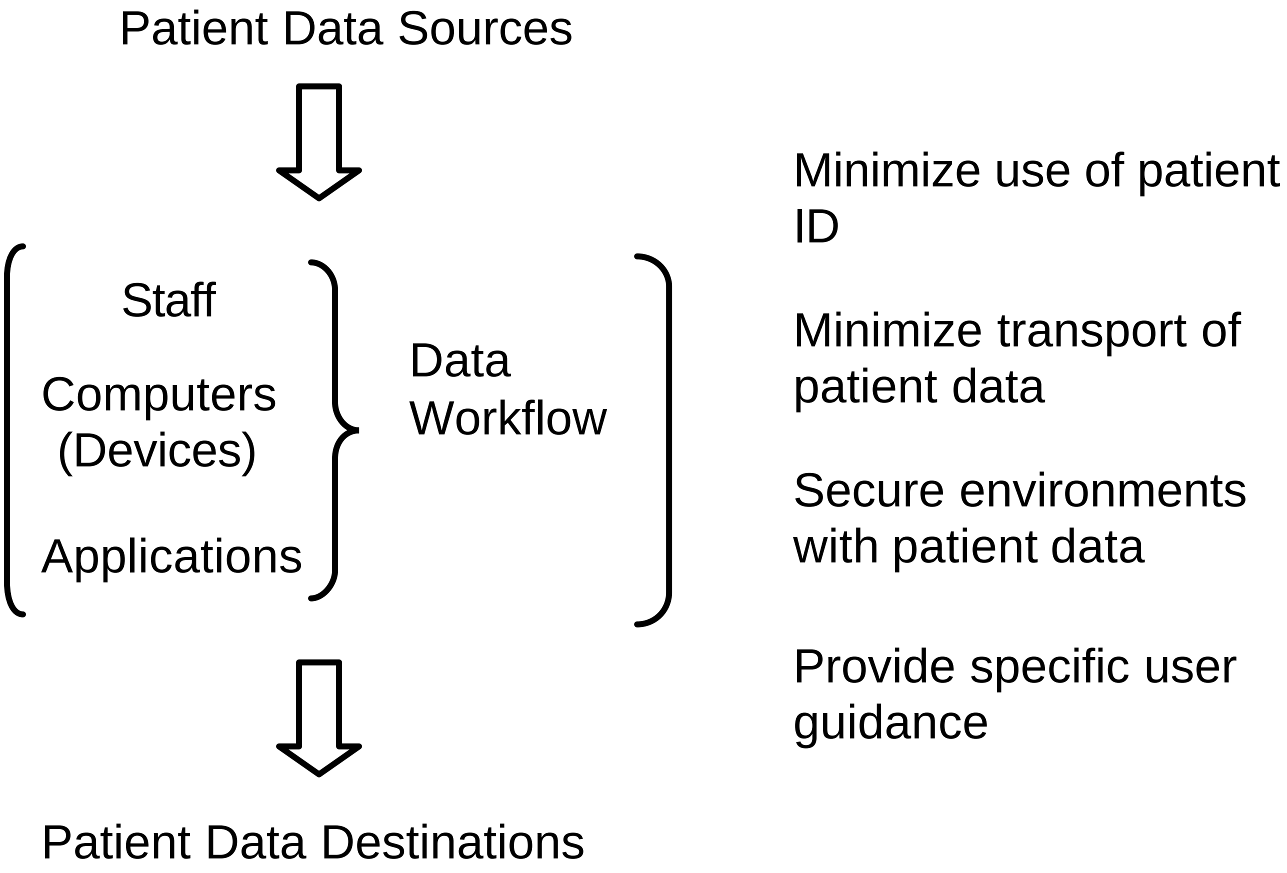
Each of these types of patient data is then traced at each stage of their processing during this activity, including any exporting of patient data to another department within HA or another organization. Specific attention is paid to identifying:

- the user(s) accessing the data,
- the applications they are using,
- the computing devices[1] on which the data is located, and
- how the data is transmitted from one computing device to another.

Having collected this information, the analysis phase then applies the Four Principles. The first step is examining the use of patient identifying information, such as HKID, in an activity and determining if its use could be reduced or eliminated. By way of example, this could be accomplished by removing the identifying information from the data exported by an application or through the use of an anonymous patient identifier. One approach to the generation of anonymous patient identifiers is described later in this chapter.

The next step is to determine if the number of computers on which the data is stored and processed can be reduced, thus minimizing the scope and complexity of any security remediation work.

[1] Computing devices includes servers, PCs, laptops, PDAs, Smart phones, medical equipment, e.g., MRI machine, and the computers connected to medical equipment.



Patient Data Sources

Staff

Computers (Devices)

Applications

Data Workflow

Minimize use of patient ID

Minimize transport of patient data

Secure environments with patient data

Provide specific user guidance

Patient Data Destinations

Once this has been accomplished, the next step is to ensure that there are adequate protections in place to protect patient data in light of the risks it faces in environment(s) in which the activity takes place. In the case of the incidents, the risks were the loss or theft of computing or memory devices with patient data. More broadly, risks could include unauthorized access to or use of patient data by HA staff, external attacks on HA computers or networks, improper use of patient data by non-HA staff, e.g., university researchers, or external attacks on data that is being exported from the HA to another organization. The protections selected may include a combination of technical, physical, and procedural measures. Based on analysis of the incidents, recommendations for an initial set of technical security measures are provided below.

Having selected and deployed the appropriate set of protection measures it is then possible to provide staff with the specific guidance they need to perform their security-related tasks properly.

Since the deployment of new technology and making changes to existing applications takes time, there may be situations in which it is necessary to adopt interim measures. While there is a great deal of diversity in HA operations and activities, it is expected that lessons learned in applying the methodology one activity will have relevance to others.

Hospital Authority’s Policy on Information Security and Privacy

The confidentiality, integrity and availability of personal information, in particular identifiable personal information, are essential to the mission of providing healthcare by the Hospital Authority, which is committed to preserving the security and privacy of personal information.

Policy Statement

The policy mandates the effective protection of security and privacy of personal information with respect to its collection, use, storage (all media), access, extraction, transmission and disposal. In particular, the Hospital Authority mandates all identifiable personal information to be accorded the highest level of security and privacy protection.

The policy ensures that personal information:

(a) be properly safeguarded to maintain confidentiality, integrity and availability,

(b) be protected according to the Personal Data (Privacy) Ordinance. The Ordinance has laid down the following data protection principles:

- Personal data should be obtained and processed lawfully and fairly
- Personal data should be accurate, up-to-date and kept no longer than necessary
- Personal data should be used for the purposes for which they were collected
- Appropriate security measures should be applied to personal data
- Information regarding personal data should be generally available
- Provide channels for data subjects to have rights of access to and correction of their personal data

(c) be accessed according to the principles of “patient-under-care” or “organisational need-to-know.

Effective procedures and measures, both administrative and technological, should be formulated, implemented and maintained to ensure policy compliance. For security and privacy violations and breaches involving personal data, an effective incident reporting and handling system must be in place to ensure speedy investigative and remedial actions in the interest of the data subjects and the community.

Relevant education and training for all employees should be regularly conducted to ensure a firm understanding of this policy, as well as the related procedures.

All HA employees, and non HA employees, who are involved in the handling and processing personal data collected by and originated from the HA, must comply with this policy, and to maintain vigilance in the protection of security and privacy of personal data. Disciplinary and legal actions may be taken against the person responsible for deliberate violations and breaches. To minimize potential and consequential damages, reporting of possible security and privacy breaches is encouraged,

Enquires

Should you have any enquiry or require any assistance regarding this policy, please contact XX: