Electronic Health Record Data Security

Dr Elizabeth QUAT
Founder & Immediate Past President, iProA
Member of Advisory Committee, eHealth Consortium
Member of Personal Data (Privacy) Advisory Committee

The 31st Asia Pacific Privacy Authorities (APPA) Meeting, 12 June 2009
Public Forum on "Electronic Health Record Sharing System from a Privacy Perspective"

About eHealth Consortium

Background

- *Founded in 2005, the eHealth Consortium is an organization that aims to enhance the quality of healthcare services through the application of medical informatics and Information and Communication Technology (ICT) in healthcare.*

Founding Member Organizations

- *Government and Quasi-government Organizations*
  - *Department of Health (DH)*
  - *Hospital Authority (HA)*
  - *Office of the Government Chief Information Officer (OGCIO)*
- *Professional Organizations*
  - *Internet Professional Association (iProA)*
  - *Hong Kong Society of Medical Informatics Ltd. (HKSMI)*

Supporting Organizations

- *Chinese Hospital Association (中国医院协会)*
- *Efficiency Unit - HKSAR*
- *GS1 Hong Kong*
- *Healthcare Information and Management Systems Society*
- *Hong Kong Academy of Medicine*
- *Hong Kong Association of Nursing Informatics*
- *Hong Kong Computer Society*
- *Hong Kong Council of Social Service*
- *Hong Kong Doctors Union*
- *Hong Kong Information Technology Joint Council*
- *Hong Kong Medical Association*
- *Hong Kong Private Hospitals Association*
- *Hong Kong Radiographer Association*
- *Information and Software Industry Association*
- *The Federation of Medical societies of Hong Kong*
- *The General Agents and Managers Association of Hong Kong*
- *The Life Underwriters Association of Hong Kong*
- *The Hong Kong Federation of Insurers*
- *The Hong Kong Institution of Engineers*

The Role of eHealth Consortium

- *Continual role in Capacity Building*
  - *Training courses for Chinese Medicine Practitioners (in progress)*
  - *Facilitating the local Master Degree course to train Health Informaticians (Baptist U, Sept 2009)*
  - *Training courses for Nurses (proposed)*
- *Initiate Pilot Projects, especially to draw participations from Private Sectors*
  - *Validation Platform*
- *Draw international expertise*
  - *eHealth Forum 2009*

Ground Works in Standardization

- *White Paper*
  - *A white paper was composed and published to increase awareness in the health care industry about the application of IT. This paper focused on the introduction of different types of standard, suggestion for data sharing and laying down the direction of usage of standard.*
  - *This paper has been posted in the OGCIO (www.ogcio.gov.hk) and the eHealth Consortium (www.ehealth.org.hk) websites.*

Capacity Building – Trainings to Private Doctors

- *Essential eHealth Skills Workshop was successful in creating awareness amongst health care workers.*
- *Among 849 attendants, 75% considered that a re-run is necessary. Overall, 66% rated the workshop good or excellent.*

Initiate Project: Validation Platform

- *Sponsored by Food and Health Bureau (FHB) and Office of the Government Chief Information Officer (OGCIO), this project will be implemented by eHealth Consortium Ltd to build a platform to test how electronic health records from various stakeholders could conform to the ultimate territory-wide standards and shared in the future.*

Awareness and Advocacy

- *IT in Health Forum 2003 & eHealth Forum 2006*
  - *provided a platform for knowledge exchange amongst IT and healthcare professionals to explore methods and share experiences on disease control a*

eHealth Forum 2009

"We Care, We Share: Creating Our eHealth Future"

www.ehealthforum2009.org

8-9 Oct (Thu- Fri)
Hong Kong Academy of Medicine
(99 Wong Chuk Hang Road)

Agenda

8 Oct	*am*	*•Pre-Conference Workshops*			
	pm	*•Forum Opening* *•Keynote Speech* *•Expert Sharing Sessions*			
		Track A: eHealth Development in Mainland China	*Track B: Health Data Standards & Interoperability*	*Track C: Confidentiality & Security*	
9 Oct	*am*	*•Keynote Speeches*			
		Track D: HIT Education & Capacity Building	*Track E: Computerized Clinical Record System*	*Track F: Improving care through eHealth*	*Track G: Disease Surveillance & Monitoring*
	pm	*•Keynote Speeches* *•Closing Plenary Session: "Way-forward of eHR in Hong Kong", Dr NT Cheung* *•Closing Remark's*			

Call for Abstracts

- *Abstracts Submission Deadline: 31 Jul 2009*
- *Topics*
  - *HK, Pearl River Delta and Greater China Electronic Health Records*
  - *Health Data Standard & Interoperability*
  - *Confidentiality & Security*
  - *HIT Education and Capacity Building*
  - *Improving care through eHealth*
  - *Disease Surveillance and Monitoring*

Current Issues…

Canada: Privacy & eHealth

- *2007 Canada Health Infoway survey*
- *Canadians reasonably confident that responsible stewardship of personal health data exists.*
  - *79% consider the health information that exists about them to be at least moderately secured.*
  - *Trust in health professionals (e.g., doctors, nurses, pharmacists) is very high; but slightly lower for other groups (e.g., administrators, government departments).*
  - *Trust levels are more mixed outside the realm of immediate health care providers (e.g., computer technicians, insurance companies, researchers).*
- ***"If you can protect my privacy, I am okay with [electronic health records]."***

United States: Privacy & eHealth

- *May 2008 CDT report on privacy and healthcare cites 2006 survey*
- *When Americans were asked about the benefits of and concerns about online health information:*
  - *80% said they are very concerned about identity theft or fraud;*
  - *77% reported being very concerned about their medical information being used for marketing purposes;*
  - *56% were concerned about employers having access to their health information; and*
  - *53% were concerned about insurers gaining access to this information.*

The Problem is Not External

- *Gartner Group:*
  - *Employees commit 70% of data breaches.*
- *2006 CSI/FBI survey:*
  - *92% of insider data thieves had negative work evaluations before breach.*
- *Univ. of Washington research:*
  - *31% of data breaches between 1980 and 2006 were committed by external parties (e.g. "hackers").*

Recent Data Breach in the US

- *More than 1.5million patient records at hospitals have been exposed by data breaches between 2000 and 2007.*
- *Data breaches are common across sectors. Medical and health care facilities contributed to 14.9% of the total 449 security breaches in 2008.*

Hong Kong Situation

- *The Hospital Authority had a series of patients' data losses with losses of electronic devices including USBs. The latest incident in May 2008 involved the loss of an unprotected USB containing the personal data of 11,000 patients.*
- *New measures has been adopted…*

eHealth Data Security

Much more than an IT project…

- *Data Security isn't solely a technical or policy issue;*
  it also involves Behaviour.
- *The protection of personal information is a personal responsibility for Each staff member.*
- *Data Security is an Ongoing Initiative, not a short-term project or goal.*
- *Privacy and Data Protection is a Culture.*

eHR Data Security

- *Key objectives:*
  - *Ensures that patients' information is kept safe from corruption*
  - *Ensures that access to patients' information is suitably controlled*
  - *Protects personal data*

Privacy should never be sacrificed!

Current Situation

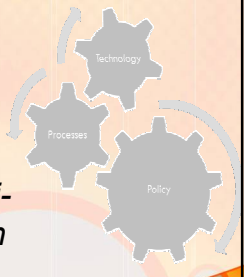
- *Technologies exist*
- *Administration Systems to be established or improved*

Current Situation – examples

- *Role-based record access controls should be further enhanced:*
  - *Patient's entire record is accessible by medical practitioners, healthcare professionals, and administrative staff working in the same public hospital.*
  - *Currently, only HIV and mental illness records are classified (i.e. accessible to professionals in a need-to-know basis)*
- *Patients are not given a choice on the disclosure level of their health records to selected doctors. Either all or none.*

Means to Enhance Data Security

1. *Security Policy*
2. *Security Audit*
3. *Privacy and Data Protection Technologies - Multi-factor Authentication*
4. *Human Issues*



1. Security Policy

- *Data classification:*
  - *defines sensitivity levels of information*
  - *apply "Need to know" policy: categorizes information so that even someone with the highest classification isn't automatically cleared to see all information at that level.*
- *Change control & management:*
  - *ensures information is appropriately protected from modification or disclosure*
  - *Effective change control can uncover:*
    - *cases of policy violation by staff; where programmes are installed or changed without following the proper notification procedures*
    - *Possible hardware failure leading to data corruption*
    - *Viruses, worms, malicious code…*
  - *Formal change control processes will help ensure that only authorized changes are made at the approved time and in the approved manner.*

Security Policy

- *Security Management Practices:*
  - *Security management planning*
  - *Employment policies & practices*
    - *Background check, Hiring & termination, Separation of duties,….*
  - *Guidelines to users on the processing, storage, and transmission of sensitive information*
  - *Risk management*
  - *Process for corporate governance to establish accountability and manage enterprise privacy risk*
  - *Procedures to implement privacy policies within operational processes, including designing and implementing measurable controls*
  - *An enterprise-wide privacy & data protection training program*
  - *Process to stay current and assess new legal regulations and legislative developments*

2. Security Audit

- *Log management*
- *Physical security assess of data centers*
- *Logical security assess of databases*
- *Access control of application and operating system*

3. Privacy and Data Protection Technologies

- *Governance Solutions (Data inventory, data classification, Digital rights management)*
- *Preventive Solutions (Data leak prevention, Identity and access management, Segregation of duties, database security /scanning, Encryption (data at rest), Encryption (data in motion))*
- *Monitoring Solutions (Content monitoring, audit logging and monitoring, intrusion detection and prevention, fraud discovery and monitoring)*

Multi-factor authentication

- *Access password*
- *Security device (e.g. Dongle)*
- *Smart card*
- *Short code by phone*
- *Biometric devices (face/fingerprint/iris/palm/voice detectors…)*

Examples:

- *Encrypted biometric access systems that allow the use of a fingerprint to authenticate an individual's identity, but do not retain the actual fingerprint;*
- *Software that allows browsers to automatically detect the privacy policy of websites and compares it to the preferences expressed by the user, highlighting any clashes;*
- *'Sticky' electronic privacy policies that are attached to the information itself preventing it being used in any way that is not compatible with that policy.*

4. Human Issues

- *Education and reinforcement*
- *Periodical backup practice/habit*
- *No download or duplication of information*
- *Safekeep of USB/transportable devices*
- *Proper disposal of PC and storage devices*
- *Careful handling of hardcopies*
- *Legislative consideration*
- *Building a culture of privacy and data protection*

Building a Culture of Privacy

- *In building a culture of privacy, an organization must:*
  - *clearly articulate privacy as an organizational priority;*
  - *communicate key privacy and security messages;*
  - *educate across the organization;*
  - *raise awareness of the importance of registering privacy incidents and breaches;*
  - *build privacy into the fabric of the organization's activities; and*
  - *make privacy information and guidance readily accessible.*

Source: eHealth Ontario

eg: eHealth Ontario - Building a Culture of Privacy

Use Innovative Marketing Approach
- Brand "Privacy Awareness": Integrate all the materials into a coherent, consistent, and instantly recognizable campaign.

Award-Winning Program

GET CAUGHT! won the following International Association of Business Communicators (IABC) awards:

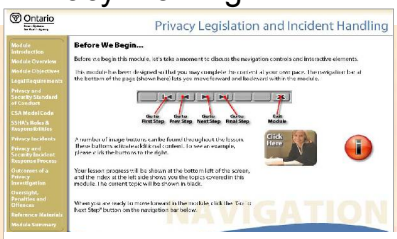
- *An international Gold Quill Award of Merit in the Other Graphic Design category;*
- *A Canadian Silver Leaf Award of Merit in the Other Graphic Design category*
- *A Toronto chapter Ovation Award of Excellence for Other Graphic Design; and*
- *A Toronto chapter Ovation Award of Merit for Employee/Member Communications*

IABC INTERNATIONAL ASSOCIATION OF BUSINESS COMMUNICATORS

WINNER 2008 OVATION AWARDS

2008 Gold Quill Award Winner Gold Quill Awards International Association of Business Communicators

Privacy Training

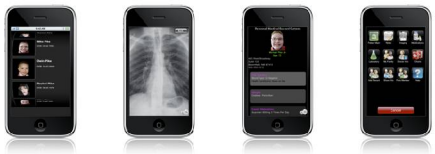


- *Online Learning Management System (LMS) with two modules for Privacy and Information Security.*
- *Mandatory for new employees: to be completed within 30 days of on-boarding date.*
- *Compliance monitoring done by PS from HR data.*
- *Non-compliance with requirement results in system lockout.*

Moving Forward…

Mobile Health Care

Your Medical Records Are Now Yours…



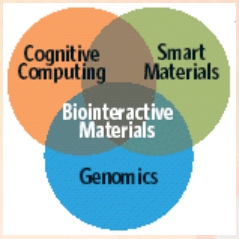
Introducing My Life Record

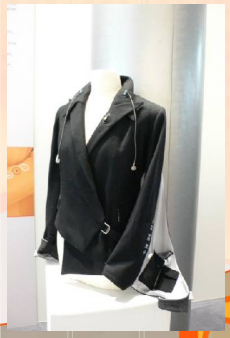
Keeping track of your medical records accurately has been a difficult, if not impossible task. Until Now. My Life Record personal medical record software allows you to keep track of your medical records like never before possible.

Everything from medical imaging, charts, medications and even lab results can now be accessed and shared all via your iPhone. Never before has your ***official*** medical record been so easy to organize and track. The days of waiting for your medical charts to arrive at your doctors office are over. The days of waiting to get results from one doctor to another are a thing of the past. My Life Record puts instant access to your entire medical chart within reach, or should we say within a touch of your screen.

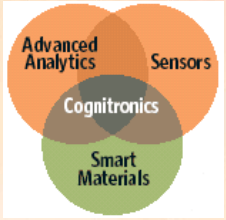
eHealth 2.0… 3.0 … 4.0…

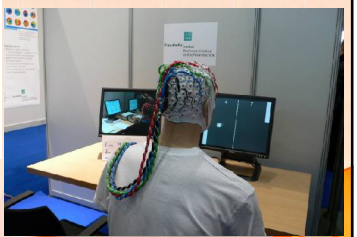
Biointeractive Materials





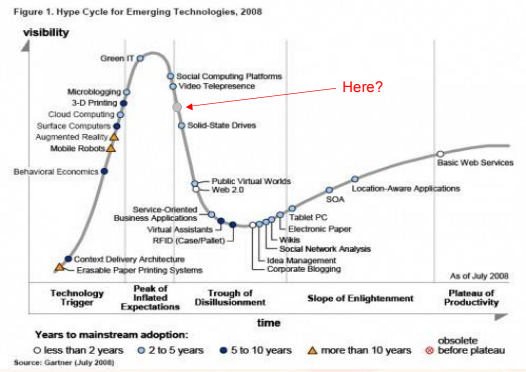
Cognitronics



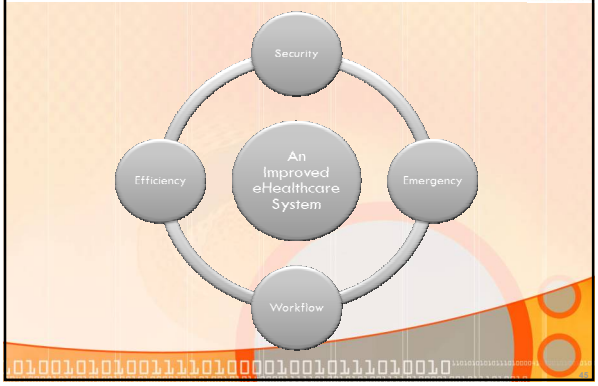


Augmented Reality

Hype Cycle: Where is eHealth?



A Fine Balance to Attain…



The World is Changing…

Can We Afford Not to Change?

We Believe….

The Basis for Technology is To Do Good,

to Solve the Problems Facing Us

Today and in the Future….

We Believe….

ICT is a Powerful Tool….

We should use it to Close the Digital Divide,

to Safe Lives,

to Eliminate Poverty,

to Tackle the Crises of the Environment,

and to Leave the Earth a Better Place.

It's Our Choices!

Be forced to Change?

vs

To Lead the Change?

Thank you!

Contact:

Dr Elizabeth Quat

email: *eq@iproa.org*

website: *www.iproa.org*

telephone: *(852) 2778 0040*

fax: *(852) 2778 0032*