Topic 2: Privacy Protection and Ensuring Security of Network Applications or Services

2.2 The Security of Electronic Medical Records (EMR)

DOH, the Executive Yuan

August 19, 2009

Agenda

1. The Vision
2. Current Situations
3. Trends
4. Strategies
5. Action Plans
6. Topics for Discussion

EMR Core Values

- Enhance medical care quality and patient safety, and reduces occurrences of medical errors
- Minimize duplicated testing, inspections, medications and appropriately utilizes medical resources
- Conserve physical storage space for medical records, and reduces environmental pollution
- Streamline administrative operations, and reduces the hospital administration costs
- It is also helpful for medical research, teaching and statistical analysis.

1. The Vision

- Provide continuous healthcare services
- A physician can obtain a patient's EMR preserved in other hospitals with patent's authorization through the NHI IC card
- Develop and maintain EMR security mechanisms to protect patient privacy

2.Current Situations (I)

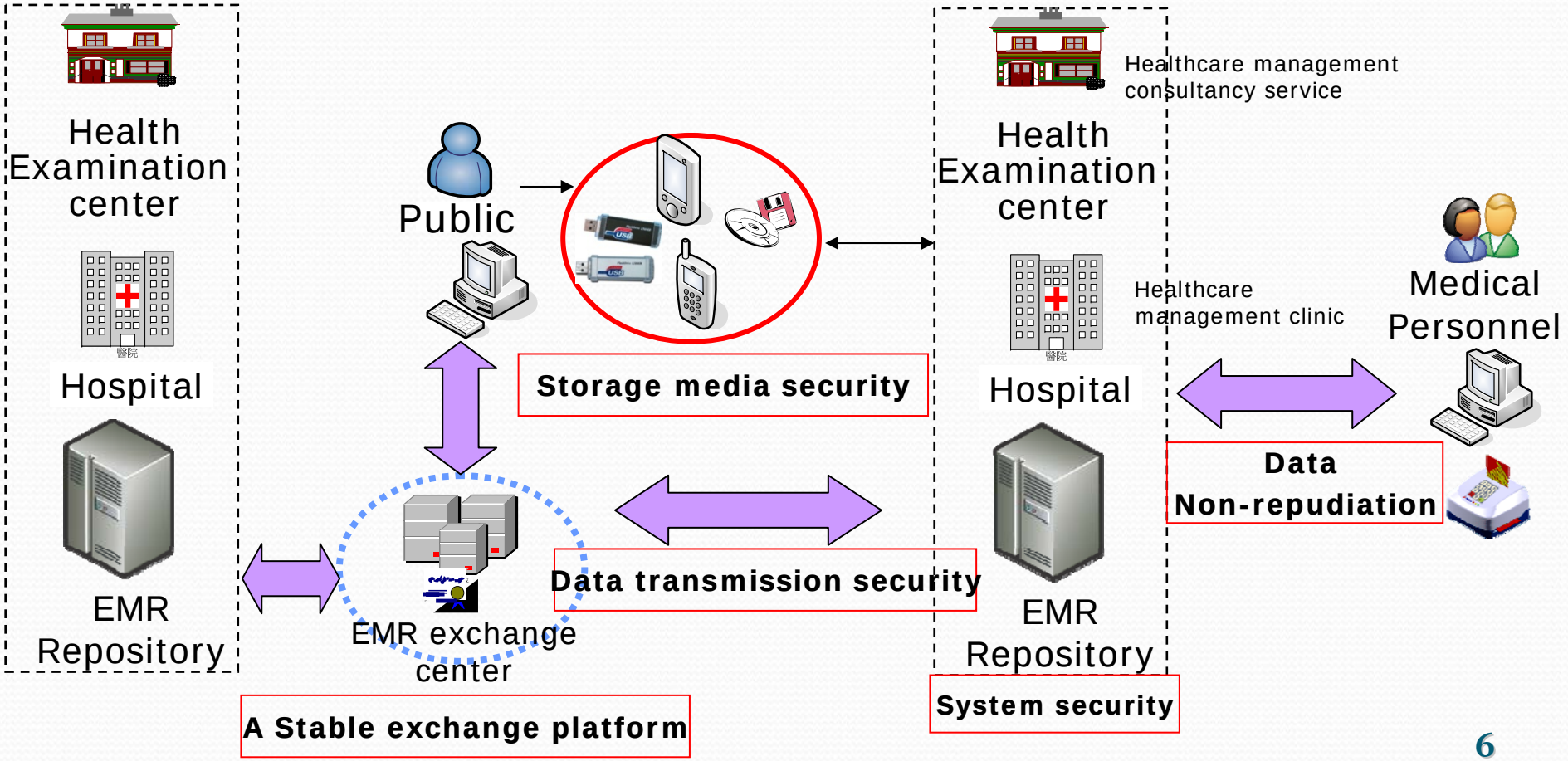
EMR Information Security

	Production & Retrieval	Storage & Management	Exchange & Sharing
Confidentiality	• Patient's privacy being infringed upon • Patients are unable to authorize the EMR access	• Patients' medical records are queried without authorization • Storages are stolen or lose	• Interception of data transmission • Unauthorized by patients • Patients have no E-signature for EMR authorization.
Integrity/ Non-repudiation	• Unable to identify the author of EMR • EMR being modified or counterfeited	• EMR being modified, counterfeited, or deleted	• EMR being modified or counterfeited • Unable to identify sender/recipient
Availability	• Error in data manipulation • System interrupts • E-signature or time-stamping is	• Medical personnel negligence • Database crash • System interrupts	• Unable to continue operation • Network being attacked by hackers

2.Current Situations (I)

EMR Information Security

EMR features: Easy to query, easy to carry, easy to store, easy to disseminate, easy to duplicate; possible information security issues



2. Current Situations (II)

Different Stakeholders' Concerns

	Possible concerns after EMR adoption
Customers (patient or public)	• Personal information may be disclosed. • Personal data may be improperly collected and used. • It is easy to duplicate and be stolen for electronic files. • The EMR's access authorization is not stipulated. • Patients have no E-signature for EMR authorization.
Hospitals & Medical Personnel	• The EMR adoption could affect work habits and consulting schedule. • Unnecessary medical disputes occurred. • Data leakage involves patients' privacy and lawsuit. • If a EMR system can't be operated due to information security events could have a serious life-threatening problem for the patient.
Professionals (information experts & suppliers)	• Improper access control of EMR • System loophole • Malicious theft by internal employees • Loss of storage media

2. Current Situations (III)

EMR & Information Security Business Opportunities

- Investment on information & communication technologies of the medical care industry:

Year \ Level		Medical centers	Regional hospitals	Local hospitals
2008	Amount	NT$71.88 million	NT$20.84 million	NT$4.79 million
	Annual growth rate	34%	14%	25%
2009		6%	1%	-1%

Data Source : Market Intelligence & Consulting Institute (MIC)

- Increasing attention on medical record security: Increase investment on hardware.
- Hospitals' investment on information security will increase 28% in 2009.

3. Trends

(1) EMR promotion projects in different countries

(2) Health information security and privacy protection regulations in different countries

(3) EMR development plans in Taiwan

(1) EMR Promotion Projects in Different Countries

Country Name	US	UK	Canada		Singapore	Korea	Australian	Taiwan
Project Name	**ARRA-HIT**	**NPfIT**	**Health Infoway**		**iN2015**	**CiEHR**		**NHIP Intelligent Medical Care**
Period	2011-2015 (5 years)	2000-2010 (10 years)	2001-2010 (10years)	-2015	-2015	2006-2013 (8 years)	2009 2010 2012-2013	2008-2010 2009-2011
Goal	Encourage physicians & hospitals to use EMR & other healthcare IT	Establish an integrated IT infrastructure & system for safe & effective transmission of healthcare information	50% of citizens have integrated EHR	100% of citizens have integrated EHR	Establish an integrated national EHR system	Everyone can use EMR and decision-making resources to improve healthcare quality, safety & efficiency at any time & in any place	Safe exchange of PHR across hospitals	80% of hospitals implement EMR & 60% of hospitals can exchange EMR
Invest-ment	US$17.2 billion (approx. NT$567.6 billion)	£6.2 billion (approx. NT$328.6 billion)	C$1.2 billion (approx. NT$36.0 billion)		US$300 million (approx. NT$9.9 billion)	Estimated to invest US$1.1 billion in 2010 (govt investment US$457 million, private sector US$620 million) (approx. NT$36.3 billion)	US$57 million, US$51.5 million, US$27 million (approx. NT$4.455 billion)	Budget for 2010 NT$937 million (non-budgetary NT$5.391 billion)

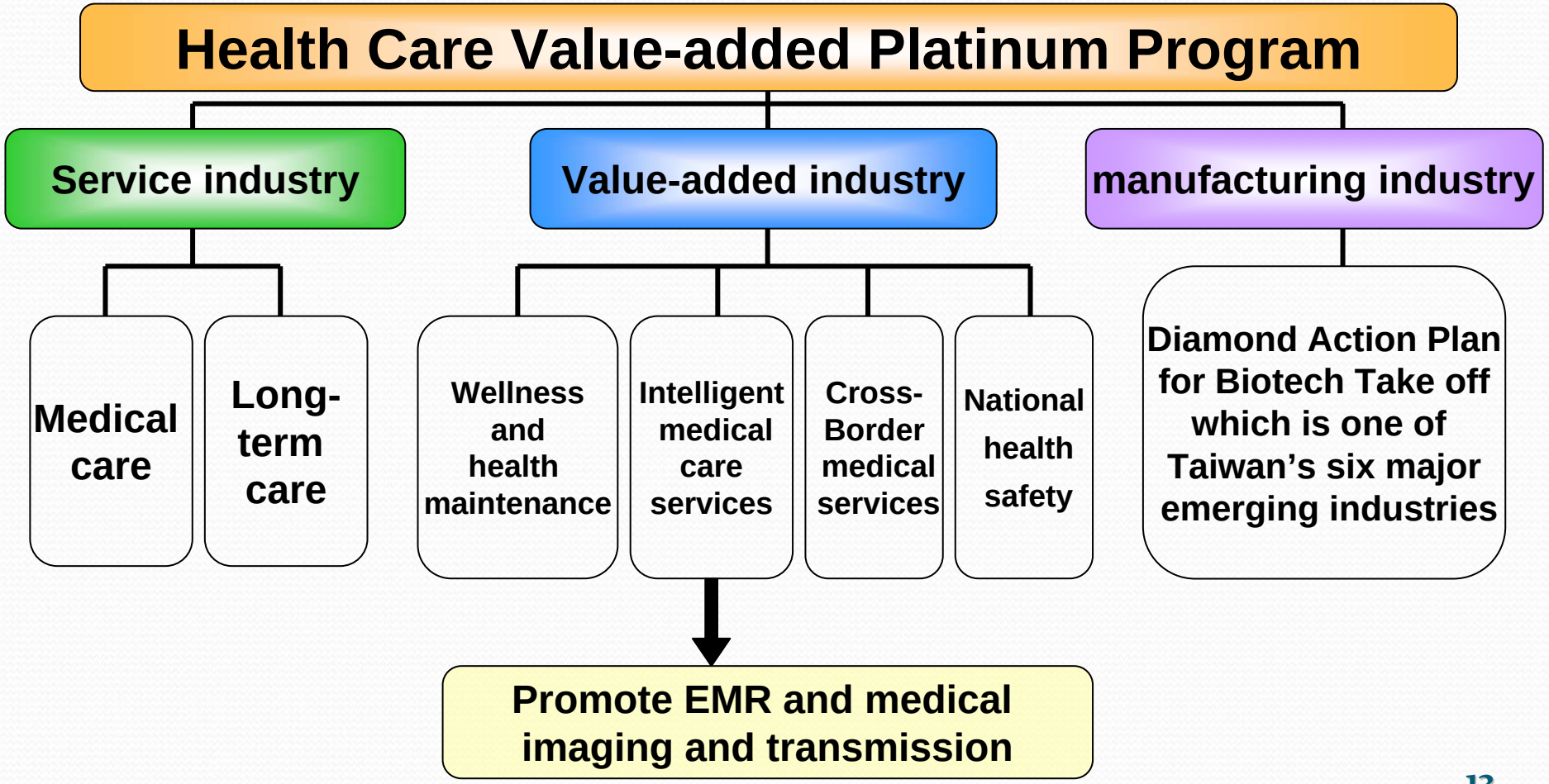
(2) Health Information Security and Privacy Protection Regulations in Different Countries (cont.)

Country Name	US	Australia
Laws & regulations	1.Health Insurance Portability and Accountability Act (HIPAA) (1996) • Security Rule (2003) • Privacy Rule: Standard for Privacy of Individually Identifiable Health Information (2002)	1. Privacy Act (1988) 2. The Privacy Amendment (Private Sector) Act (2000) 3. Guidelines on Privacy in the Private Health Sector (2001) 4. Guideline under Section 95 of the Privacy Act (1988) 5. Draft National Health Privacy Code (2002)

(2) Health Information Security and Privacy Protection Regulations in Different Countries

Country Name	Canada	New Zealand	Taiwan
Laws & regulations	1. Privacy Act (1983) 2. Personal Information Protection and Electronic Documents Act (2000)	1. Privacy Act (1993) 2. Health Information Privacy Code (1994)	1. Computer-Processed Personal Data Protection Act 2. Article 316 of Criminal Law 3. Article 23 of Physician Act 4. Article 27 of Nursing Personnel Act 5. Article 49 of Medical Care Act 6. Grand Justices Meeting Interpretation No.603

(3) The Relationship Between Taiwan's EMR Development Plans and the "Health Care Value-added Platinum Program"



(3) Taiwan's EMR Development Plans– Intelligent Medical Care Services

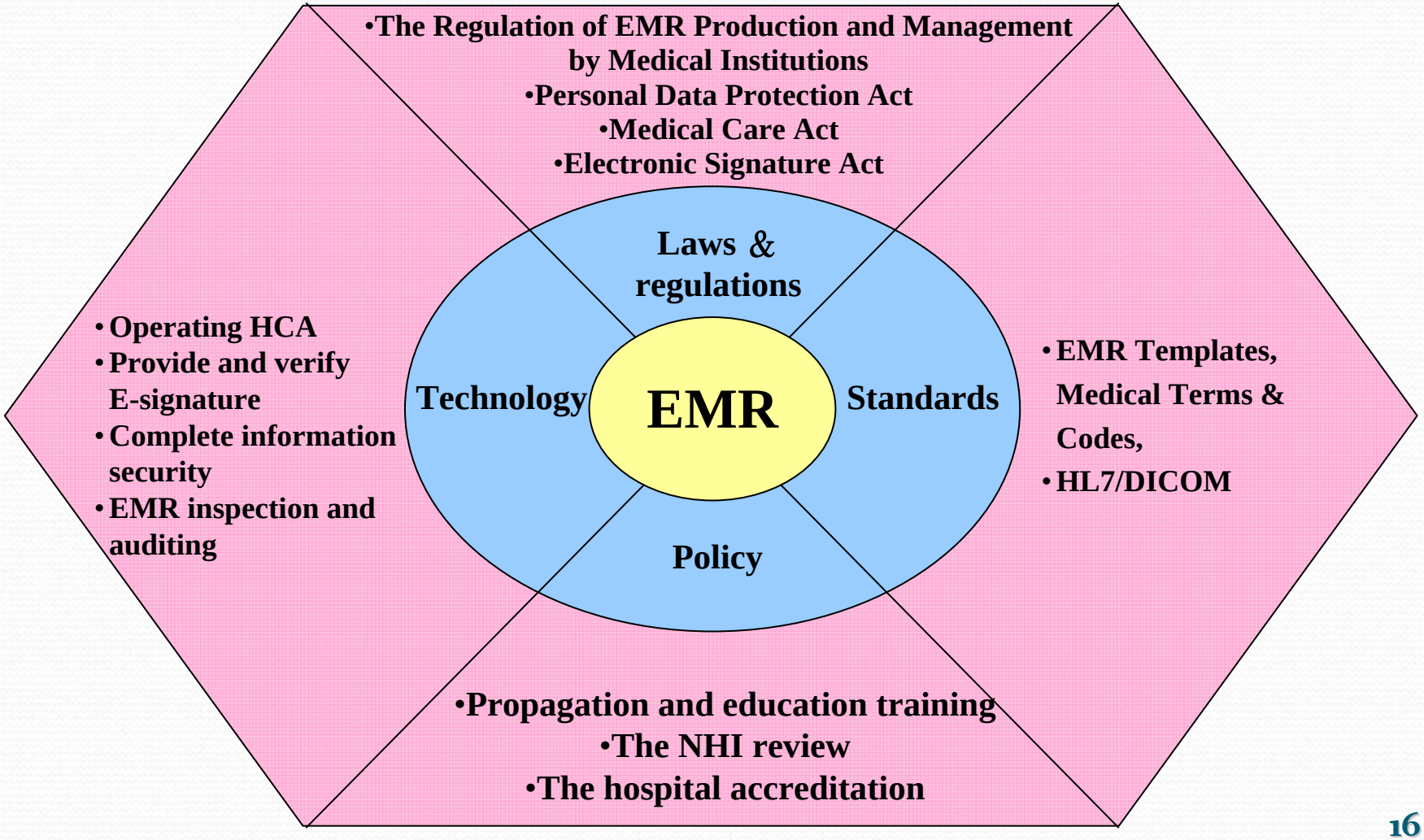
- **Objectives**
  - In 3 years (by 2012), 80% of hospitals in Taiwan (400 hospitals) will have adopted EMR for medical imaging and report, test reports and medication records with at least 60% of hospitals with inter-hospital exchange.
  - In 5 years (by 2014), all hospitals will have adopted EMR and had EMR exchange systems.

(3) Taiwan's EMR development plan– Funding Requirements of Intelligent Medical Care Service

(Unit: Thousand NT$)

Work items	2010	2011	2012	Total
1. Establish Taiwan's EMR development regulations and infrastructure	99,000	93,000	68,000	270,000
2. Enhance hospital information development and integrate it with the hospital accreditation and NHI review	5,000	4,000	2,000	11,000
3. Encourage and subsidize hospitals with computerization of medical care operation and medical records	596,000	2,513,500	2,559,500	5,669,000
4. Promote inter-hospital EMR exchange	0	30,000	70,000	100,000
Total	700,000	2,640,500	2,699,500	6,040,000

4. Strategies - Four Dimensions



4. Strategies

To resolve relevant issues related to information security of EMR from the technical, legal, policy and standards sides.

Technical side	●Provide identity authentication, time-stamping and encryption functions ●Provide a double identity authentication mechanism ●Elevate information security level
Legal side	●Improve EMR security & privacy protection through legislations. ●Specify EMR must comply with information security laws and regulations and timely amend to adapt to technological development
Policy side	●Implement inspection and auditing of EMR ●Provide identifiable logos for the physicians and patients ●Provide hospitals incentives through the hospital accreditation and NHI review ●Training of information security talents
Standards side	●Formulate standard EMR format ●Establish an EMR standard maintenance mechanism and management system

5. Action Plans

Technical side	●Provide identity authentication, time-stamping and encryption functions ●Provide a double identity authentication mechanism ●Elevate information security level	**1.Expand HCA certification applications** **2.Establish an EMR exchange center with the double identity certification** **3.Encourage hospitals to pass the accreditation of information security management system**
Legal side	●Improve EMR security & privacy protection through legislations. ●Specify EMR must comply with information security laws and regulations and timely amend to adapt to technological development	**1.Continue to amend the Regulation of EMR Production and Management by Medical Institutions** **2.Discuss and formulate EMR privacy protection laws and regulations**
Policy side	●Implement inspection and auditing of EMR ●Provide identifiable logos for the physicians and patients ●Provide hospitals incentives through the hospital accreditation and NHI review ●Training of information security talents	**1.Formulate the EMR inspection mechanism** **2.Operate the EMR Certification Center and issue certified EMR logos** **3.Add a "information management" item to the new hospital accreditation** **4.Train information security personnel for hospitals**
Standards side	●Formulate standard EMR format ●Establish an EMR standard maintenance mechanism and management system	**1.Formulate common and interoperable EMR fields standards** **2. Establish a standard EMR management system and provide the latest version standard through a maintenance mechanism**

5. Action Plans - Technical Side

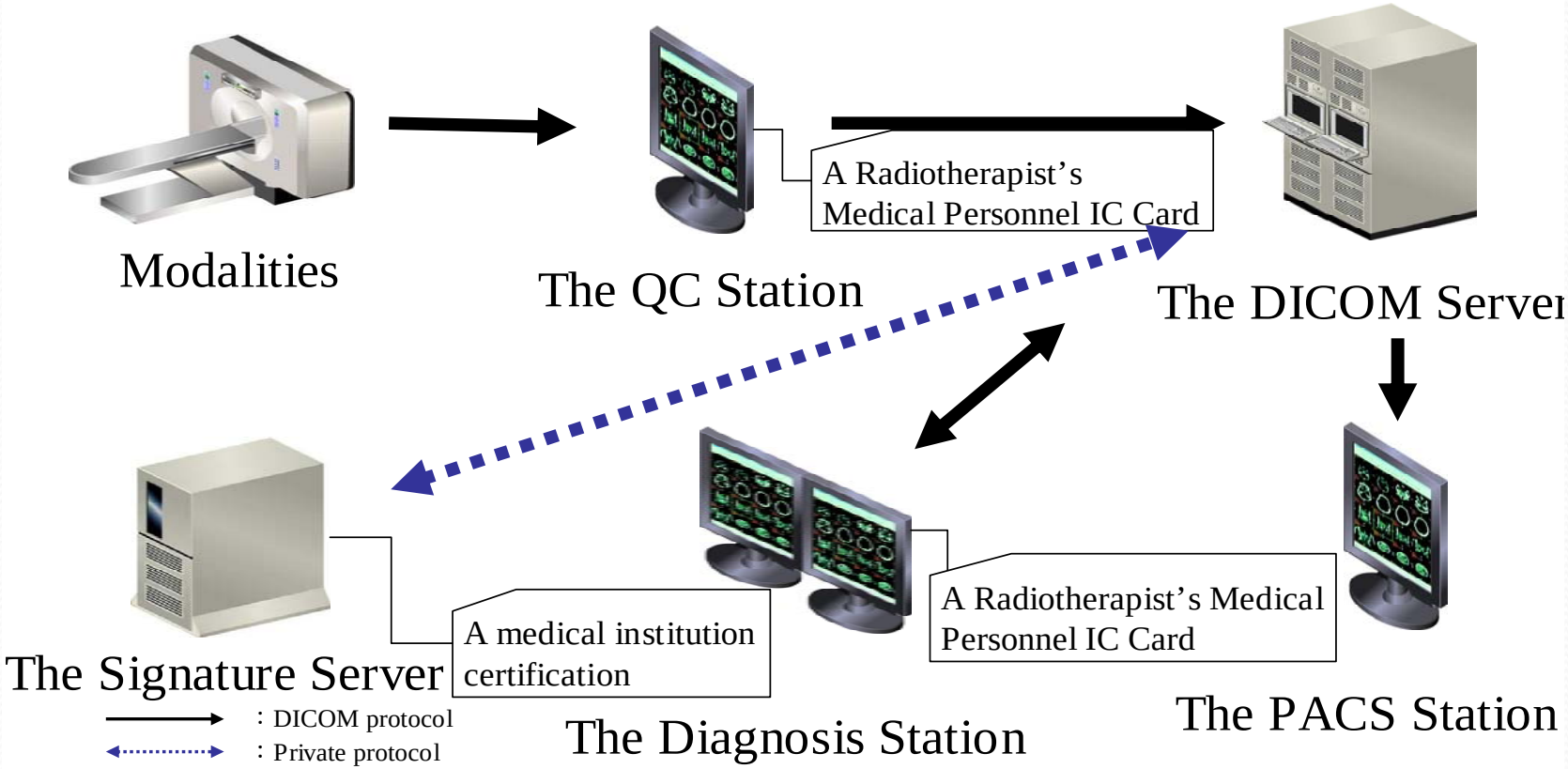
(1) Expand HCA Certification Applications

Encourage & subsidize hospitals to adopt EMR

- Provide the E-signature to replace the autograph or seal on medical records in accordance with the law for verification of a signer's identification.
- Improve EMR security through the certification encryption, and protect patient's privacy and integrity of medical records through accessing medical records with authorized certification decryption.
- Use the time-stamping as a proof of time for EMR's send/receive and reinforce the non-repudiation of the send/receive.

KPI	Percentage of hospitals which will have adopted EMR: 2010, 20 % (approx. 100 hospitals), 2011, 50 % (approx. 250 hospitals), 2012, 80 % (approx. 400 hospitals)

HCA Applications in a Medical Image Transmission System



5. Action Plans - Technical Side

(2) Establish an EMR Exchange Center with the Double Identity Certification

- Establish an EMR exchange center
  - EMR are stored in various hospitals.
  - The exchange center provides index for EMR query.
  - Physicians in different hospitals query patient's EMR via the exchange center.
  - The Double identity certification (a patient's health insurance IC card & a medical personnel IC card) ensures patient's privacy with authorization.

KPI	2009: Establish an image exchange center 2010: Expand the image exchange center, which is for 29 DOH hospitals to exchange medical records, into an EMR exchange center

5. Action Plans - Technical Side

(3) Encourage Hospitals to Pass the Accreditation of Information Security Management System

- For achieving publicly-accredited information security level and ensuring security of medical records to protect public privacy and benefits, the DOH counsel and subsidize hospitals to pass the certification of ISO 27001:2005 information security management system.

KPI	The 9 % of hospitals will be counseled and pass the certification of ISO 27001 information security every year commencing in 2009.

5. Action Plans - Legal Side

(1) Continue to Amend the Regulation of EMR Production and Management by Medical Institutions (cont.)

- For giving EMR legal status, Article 69 of Medical Care Act was added on Apr. 28, 2004.
- Promulgated “the Regulation of Production and Management of EMR for Medical Institutions” on Nov. 24, 2005, hereafter EMR conforming to this regulation no longer requires to print out medical records in paper.
- It is the only regulation which medical institutions must comply with if they want to adopt EMR.
- The purpose of this regulation is to promote self-management and continuous improvement EMR by hospitals.

5. Action Plans - Legal Side

(1) Continue to Amend the Regulation of EMR Production and Management by Medical Institutions

- **Article 3** specifies the installation of EMR system shall conform to information security regulations.
- **Article 6** specifies the identify certification of the E-signature in EMR shall be issued by the central competent authority.
- **Article 7** specifies medical institutions shall post the commence date and scope of EMR adoption in noticeable places and report to the competent county (city) authorities.

5. Action Plans - Legal Side

(2) Discuss and Formulate EMR Privacy Protection Laws and Regulations

- Taiwan laws seldom involve the privacy, but the essence of privacy is consistent with other regulations. e.g. protection of reputation, credit and secret.
- The DOH will refer to US Health Insurance Portability & Accountability Act (HIPAA) in the future and discuss the necessity of a centralized legislation on medical care information privacy.

5.Action Plans - Policy Side

(1) Formulate the EMR Inspection Mechanism

- The EMR adoption shall be in accordance with Article 26 of Medical Care Act, and medical institutions shall not reject the inspection by competent authorities.
- Use the ISO 27001 PDCA guideline for formulating inspection items in accordance with the Regulation of EMR Production and Management by Medical Institutions.
- Carry out irregular and post inspection in hospitals which have declared to adopt EMR and urges them to continuously improve.

KPI	To complete formulation of the EMR inspection mechanism by 2009.

5. Action Plans - Policy Side

(2) Operate the EMR Certification Center and Issue Certified EMR Logos

- Verify medical institutions' EMR for compliance with the Regulation of EMR Production and Management by Medical Institutions.
- Provide certified EMR logos for public to identify which hospitals have adopted certified EMR and to promote hospitals to adopt EMR.
  - Set up a national EMR certification website
  - Design the certified EMR logo and propagate its meaning and honor
  - Provide hospital the EMR certification (including re-certification) service
  - Train EMR certification manpower and provide consultancy services

KPI	To commence the operation of the EMR Certification Center by 2010.

5.Action Plans - Policy Side

(3) Add a "Information Management" item to the New Hospital Accreditation

- Establish a safe and patient-centered medical care service mechanism; the DOH has commenced the hospital accreditation across Taiwan since 1988 and launched the new hospital accreditation since 2007.
- **The latter** added information management accreditation item: Requires hospitals to complete information management mechanism for ensuring the confidentiality, safety, availability and integrity of information.
- Design a accreditation scoring mechanism according to the result of accreditation for providing hospitals incentives to adopt EMR

5.Action Plans - Policy Side

(4) Train Information Security Personnel for Hospitals

- Foster information security consciousness for medical personnel to minimize operation errors
- Training Courses are held to educate hospitals' information security personnel and then encourage them to acquire Lead Auditor (LA) qualifications of ISO 27001.
- Hospital information security seminars are held to elevate consciousness and capabilities of hospitals' internal personnel in information security and privacy protection

KPI	Continue to offer one quota for ISO27001 LA training to each hospital every year and hold 80 hospital seminars.

5.Action Plans - Standards Side

(1) Formulate Common and Interoperable EMR Fields Standards

- For requirement of inter-hospital EMR exchange, the DOH specified the regulation of E-signature and will formulate 108 standard EMR templates.
- In the future, the DOH will define the mandatory templates according to the specification of EMR exchange for proving appropriate EMR content, so as to minimize infringement risks of patients' privacy.

KPI	To complete 108 standard EMR templates by 2009.

5.Action Plans - Standards Side

(2)Establish a Standard EMR Management System and Provide the Latest Version Standard through a Maintenance Mechanism

- After formulating and verifying EMR templates, composers need to register them through a standard EMR management system for effective management templates.
- Follow six steps which are proposal, draft, announcement, review, voting and issue in establishing maintenance mechanism to ensure integrity and correctness of domestic standard EMR templates.

KPI	Establishes a standard EMR templates management system by 2009.

6.Topics for Discussion -

Topic 1

Question:

How can a patient give consent for reading, transmission and exchange of whole or part of EMR, and he/she won't be worried about the issue of information security?

Explanation:

In recent years, public has more concerned with the personal medical care information privacy protection, particularly those with special diseases (eg. AIDS and mental disorder), VIP patients or politicians are stringent for privacy protection since data leakage may affect a person's schooling, employment, medical care and living rights and benefits, and could even lead to national, social and political turmoil and insecurity.

Target:

Hospitals have adopted EMR for paperless and filmless medical records, but there are still some difficulties in generating electronic consent letters by patients. Can NHI IC cards provide patients with the electronic signature mechanism？ Can we combine the medical personnel IC card with the NHI card in order to meet the goal of "cards reduction"？

6.Topics for Discussion -

Topic 2

In view of citizens' concerns in privacy regarding the medical care information and benefit to human well-being, is it necessary to formulate a specific law that is similar to US and New Zealand for privacy of medical care information and security protection?

Thank you for your attention