



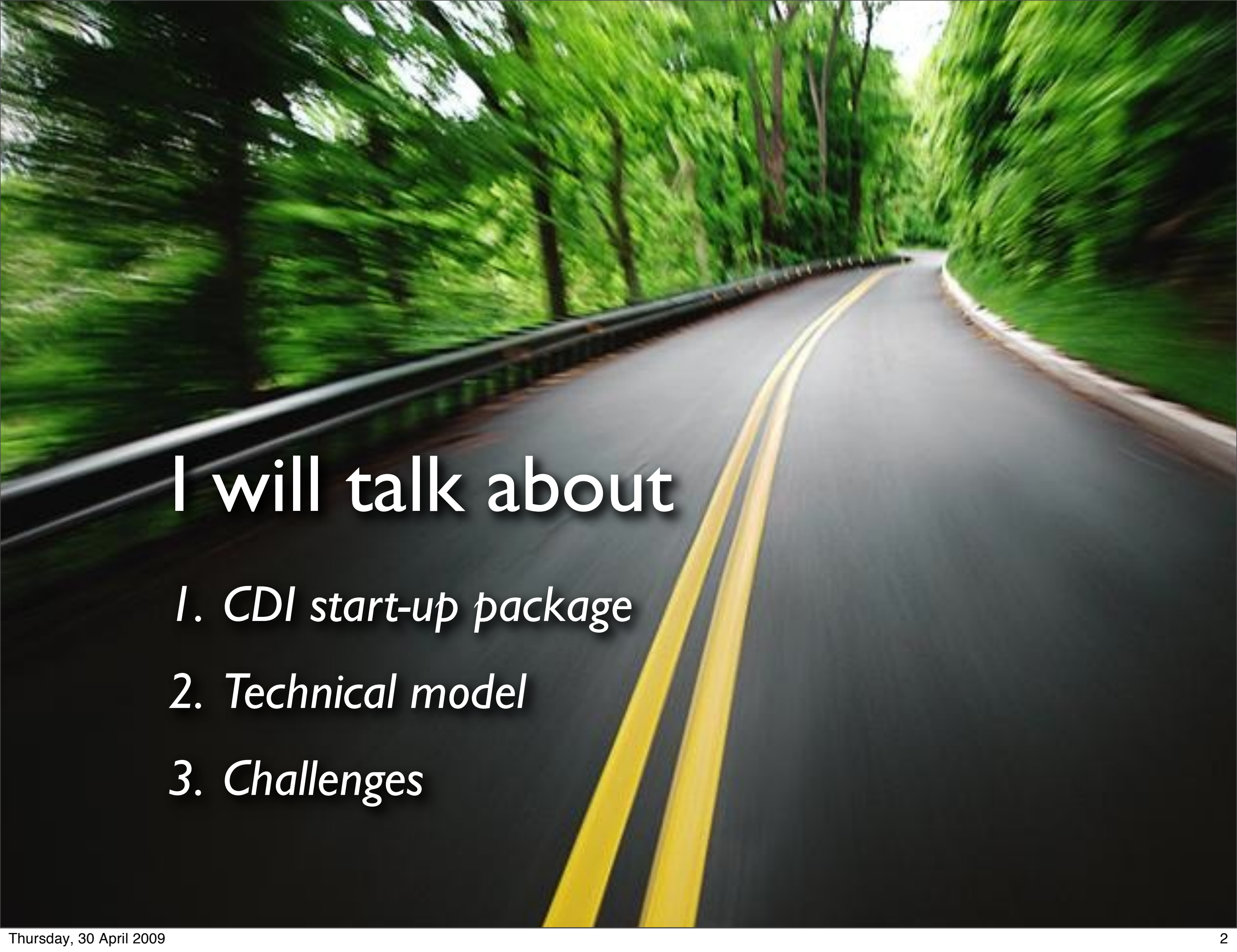
CDI Sharing to ICU CIS seminar

on 22-April-2009

by James TAN

Health Informatician

HAHO ITS



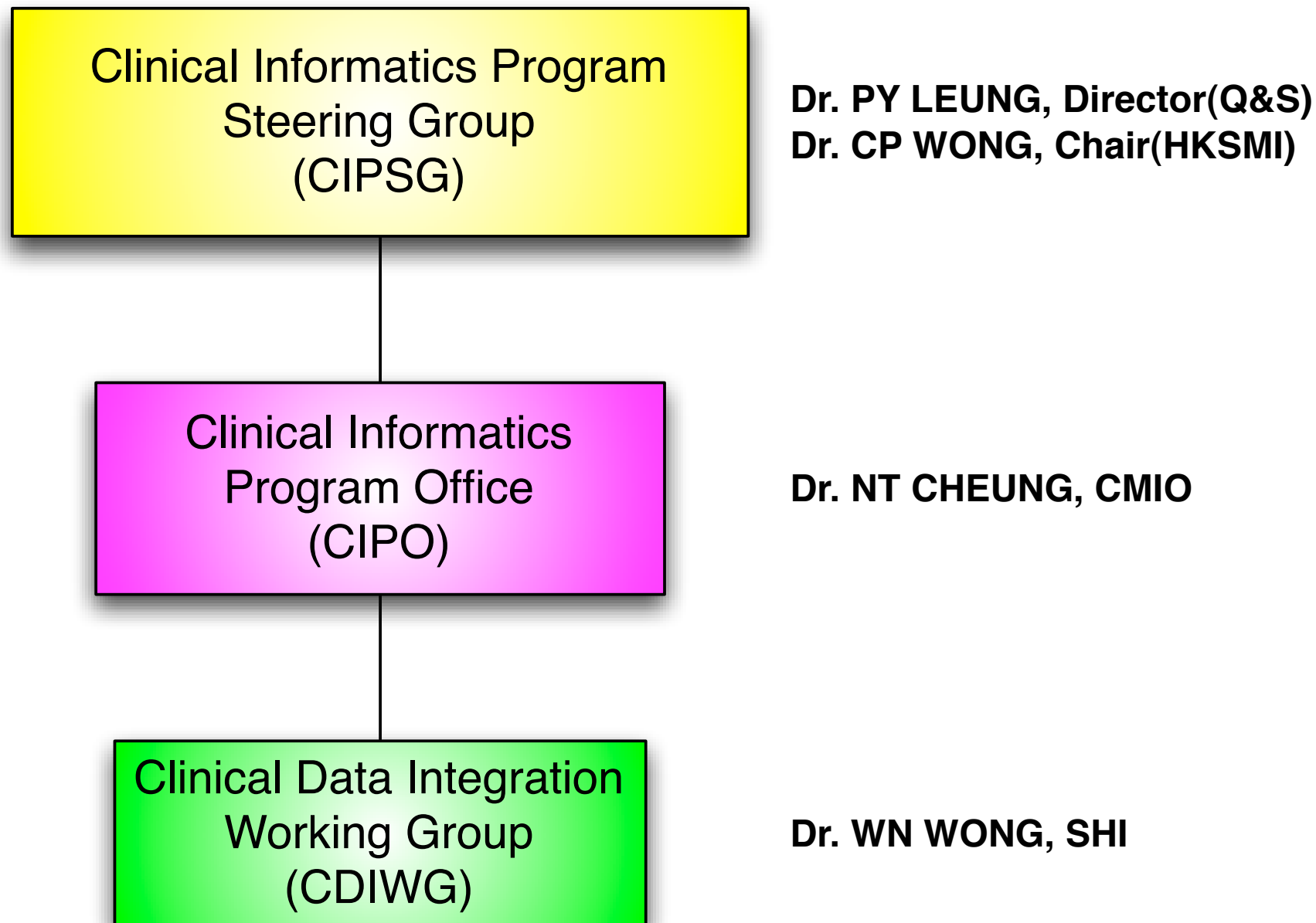
I will talk about

- 1. CDI start-up package*
- 2. Technical model*
- 3. Challenges*

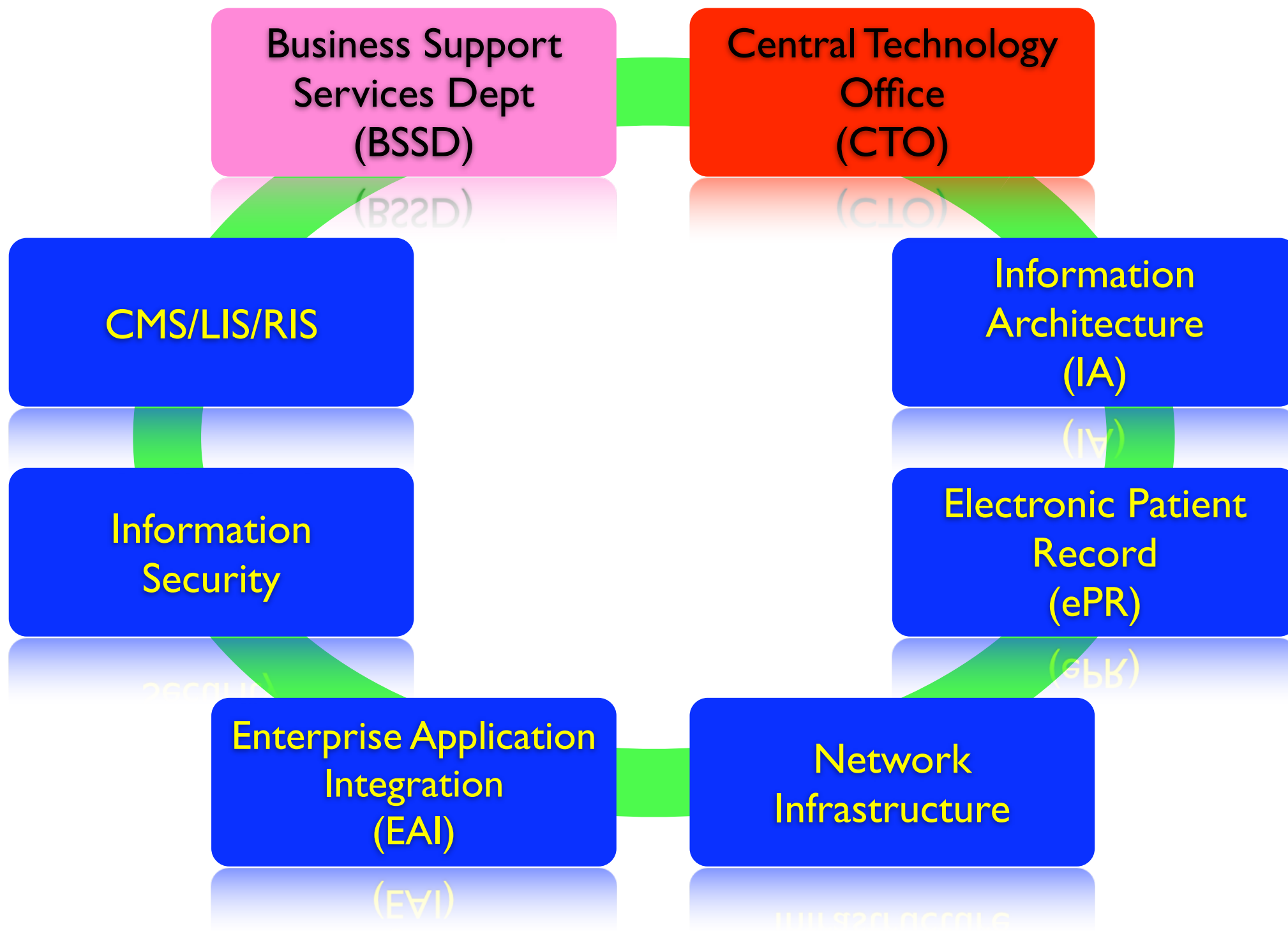


Clinical Data Integration (CDI) WG

Governance



Membership



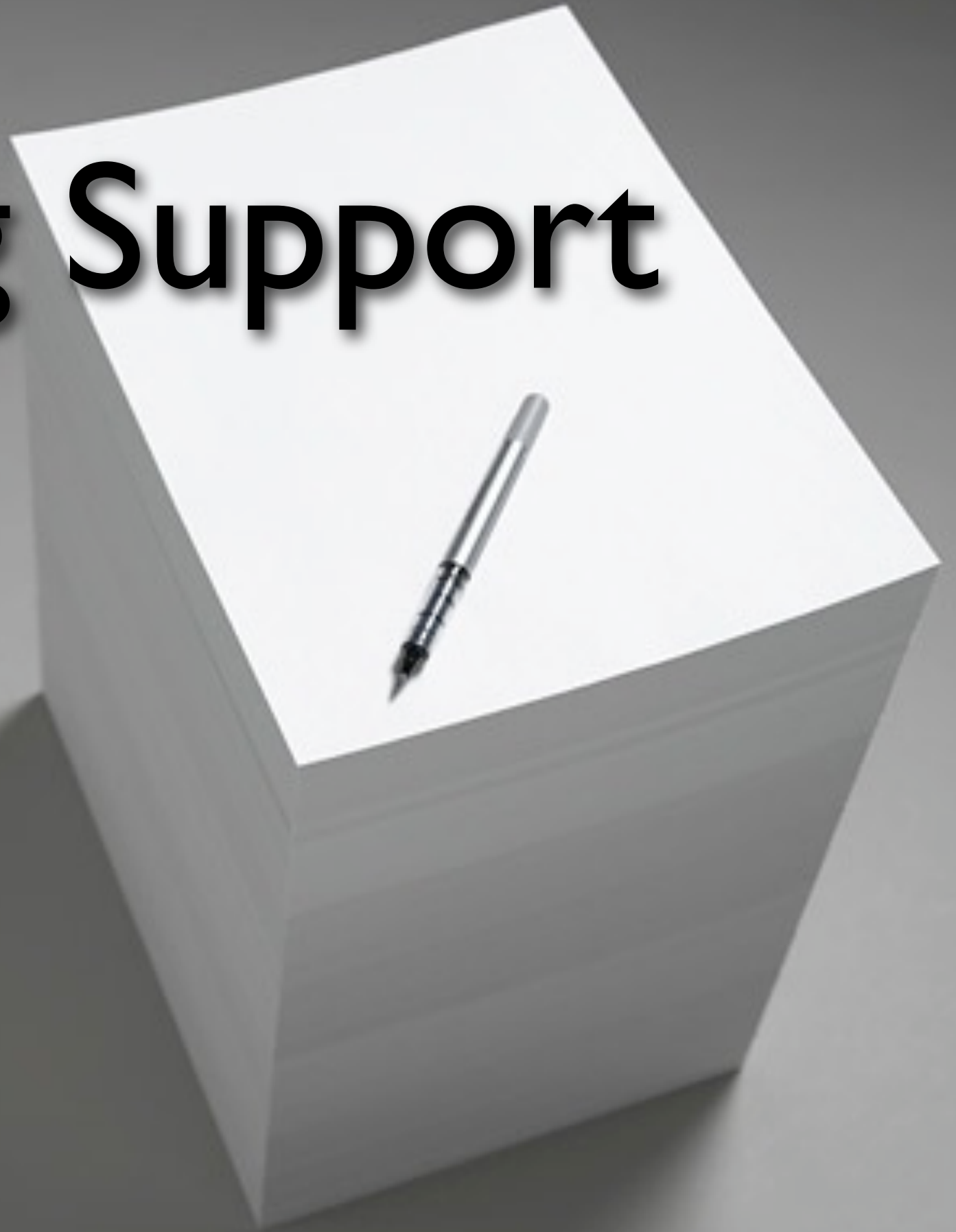
CDIWG

- ❖ Established in Oct-2007
- ❖ To recommend clinical and operating standard and procedures for clinical data interfacing (CDI)
- ❖ To review and prioritize CDI requests
- ❖ To advise on CDI implementation issues
- ❖ To report to CIPO & CIPSG

CDI Start-up Package



Tendering Support



(I) Consolidated Tender Recommendations

Generic Clauses

- (1) IT security
- (2) Network connectivity
- (3) Data security
- (4) Application security
- (5) Equipment maintenance
- (6) Clinical data exchange
- (7) Technological advancement

Specialty Requirements

- (a) Anaesthesia (e.g. Pre-, Intra- & Post-op, SSI)
- (b) ICU (e.g. APACHE)
- (c) Cardiology (e.g. PCI audit)



Prioritization

Project Prioritization

Principle	Score
1. Benefits	Low 1 ~ 3 High
2. Technical Readiness	Low 1 ~ 3 High
3. User Readiness	Low 1 ~ 3 High
4. Data Readiness	Low 1 ~ 3 High
5. Risk	High -3 ~ -1 Low
6. Alignment	Low 1 ~ 3 High
7. Cost	Low 1 ~ 3 High
8. Innovation	Low 1 ~ 3 High

CHECKLIST



Healthiness Checklist

Security Requirements for Medical Systems Installed in HA					
	Items for Verification with Vendor	Complied (Y/N)	Reviewer	Agreed by (Vendor)	Remark
Data Security (Review in regular basis)					
1	Confidential data downloaded from the medical system to end-user devices should be encrypted		Cluster IT	e.g. Philips	
2	Confidential data transferring between the medical systems and other HA IT systems should "preferably" be encrypted		HAHO EAI		<i>draeger, ge, philips, siemens, agfa (eoi on their capability)</i>
3	Confidential data stored within the medical systems should "preferably" be encrypted		Cluster IT		
4	Confidential data stored in backup storage should be encrypted		Cluster IT		
5	Confidential data must not be exported for any usage other than clinical care in HA		End-user department		
Application Security (Review in regular basis)					
1	The application should support role-based access control		Cluster IT		
2	The application should employ prevalent authentication mechanism at reasonable safety level		Cluster IT		
3	The application should apply network level encryption		Cluster IT		
4	The application should provide health-checking information		Cluster IT		
5	The application should keep audit logs		Cluster IT		
6	Conformance to HA's SDLC Application Security Guidelines		Cluster IT		
7	Conformance to HA's Web Application Security Design Guidelines?		Cluster IT		
Network Security (Review in regular basis)					
1	The medical systems network should not have any network connection to external parties		Cluster IT		
2	The medical systems network should connect to the HA Network through the Firewall located in the Hospital Data Centre		Cluster IT		
3	The medical system network should use IP addresses as assigned by HA		Cluster IT		
4	Only the authorised network traffic is permitted between the medical system network and HA network		Cluster IT		
Server Security (Review in regular basis)					
1	Vendor should implement the server security as described in the		Cluster IT		

- Data security
- Application security
- Network security
- Server security

- Client / Desktop security
- Incident reporting
- Vendor maintenance

Non- Compliance



Noncompliance form

Attn:	HO ITD IS4 team for Clinical Data Integration Working Group (CDIWG)	Enquiry:	2711 7959 / 2711 4231
Address:	4/F, Block A, Multicentre, PYNEH	Email:	HA ITS Clinical Data Integration WG

Hospital Authority
<u>Noncompliance Form For Clinical Data Integration</u>

Section I: Service Requirement (To Be Completed By Requester)

Service Description:			
Hospital:	Dept/Specialty:	Location:	
Ext. System Provider:	Application Name:		
Project Kick-off Date:			
HA Systems Involved:			

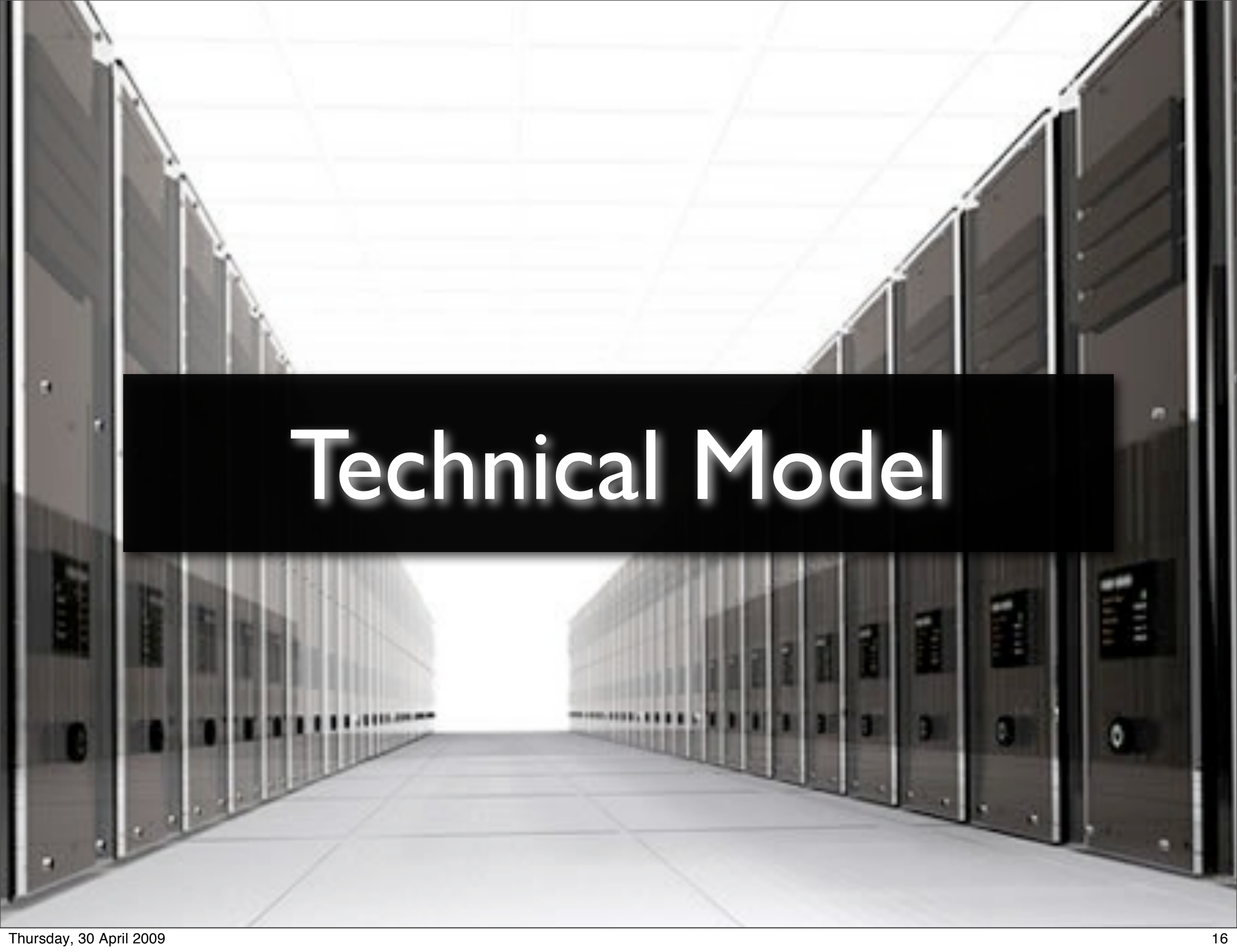
Noncompliance description and reason :

	Acknowledge By (Clinical User)
Signature:	_____
Name:	_____
Hosp./Rank/Post:	_____
Contact Phone No.:	_____
Date:	_____

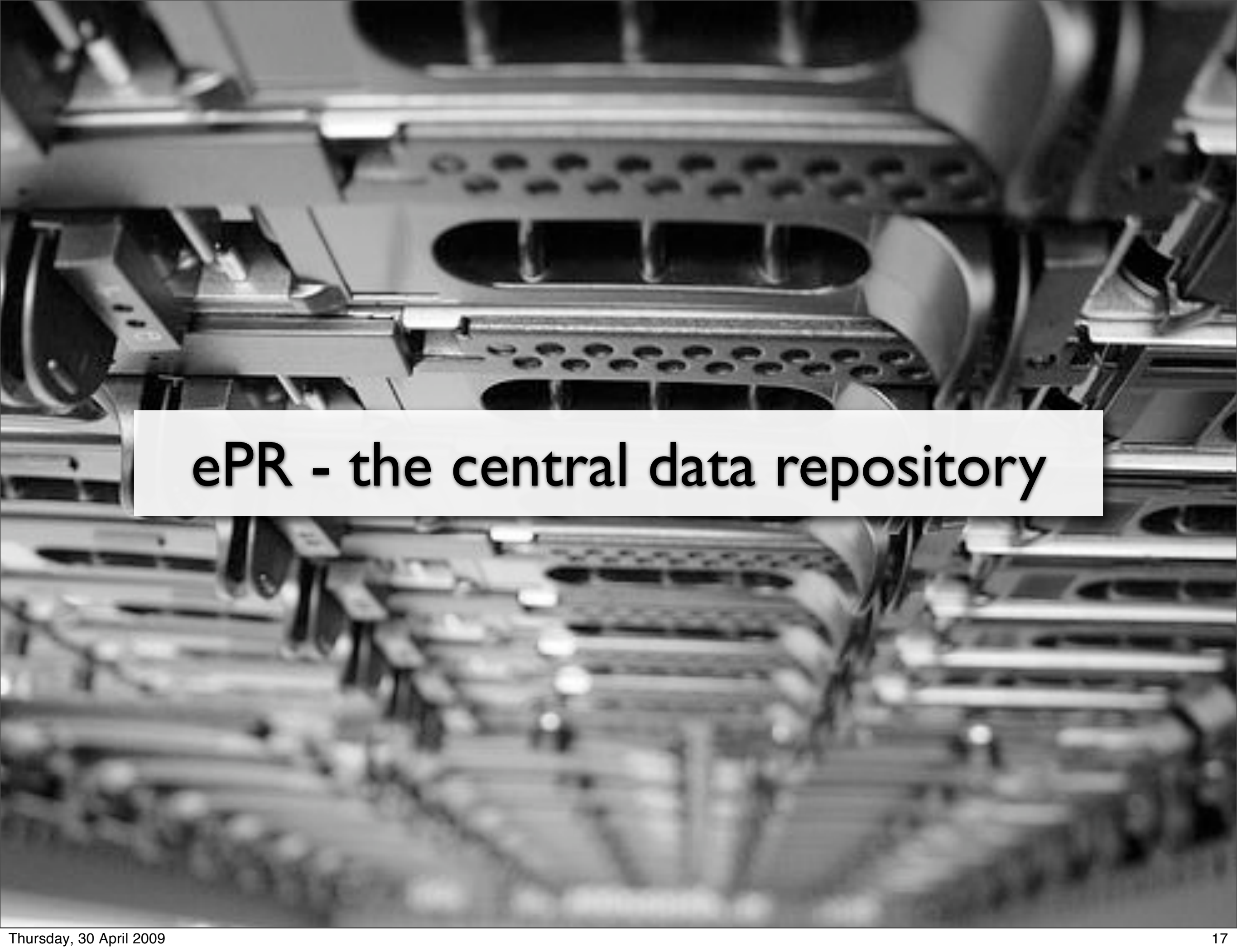
Section II: Official Use Only (To Be Completed By Secretary of CIWG)

Ref. Num.	_____	
Reason:	_____	
Signature:	_____	
Name:	_____	
Date:	_____	

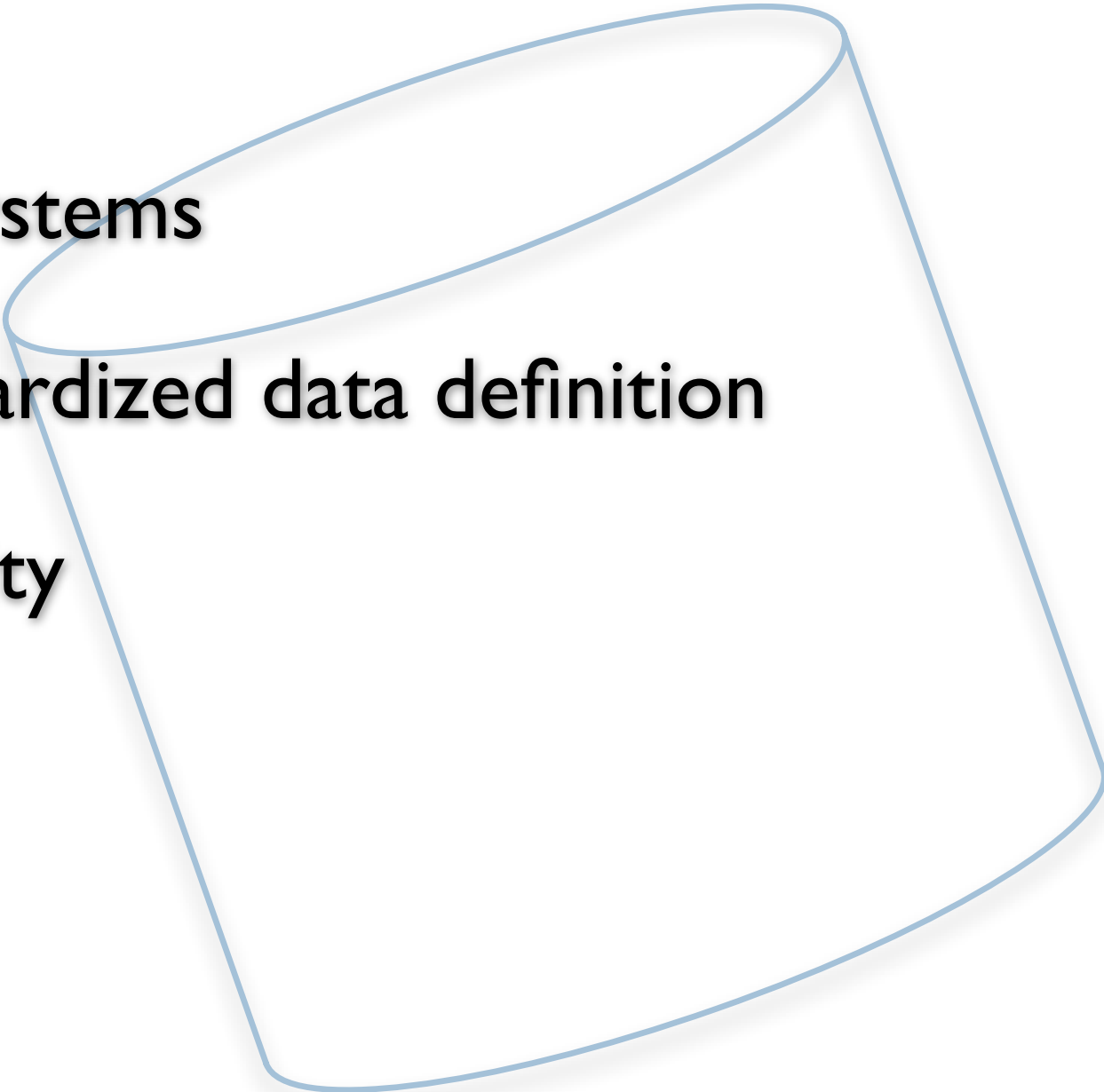
Date:	_____	
ISWG:	_____	



Technical Model



ePR - the central data repository

- 
- ❖ **Connected to all HA systems**
 - ❖ **Corporate-Wide standardized data definition**
 - ❖ **Robust with high capacity**

HL7 Data Exchange

via

Enterprise Application Integration (EAI)



How does HL7 look like?

```
MSH|^~\&|EDI|CMC|PMS|CMC|20070902000027||ADT^A08|20070902000023|D|2.3.1|||ER|ER|HKG|ASCII|ENG
EVN||20070825000024.853|20070825000024
PID|1||HKID:A1234560~PKey:11223334||CHAN^TAI MAN^AAAA^I:11111:22222:33333||19170101|M||CH|1,2,33 TAI NAM ST^SSP||^AAAA^11221122|||M| |||||||||||N
NK1|1|LAM, HO HO|||DA|^ |^AAAA^97979797
PV1|1|I|CCU^CCU^03||| ||||||||||| HN070000008||| |||||||||||20070810005900
```

```
MSH|^~\&|EDI|CMC|PMS|CMC|20070902000028||ADT^A08|20070902000024|D|2.3.1|||ER|ER|HKG|ASCII|ENG
EVN||20070826120012.833|20070826120012
PID|1||HKID:UC0001122~PKey:66655544||CHEUNG^TAI MING||19780101|M||CH|,M,111 CASTLE PEAK RD^SSP|||M| |||||||||||N
NK1|1|CHAN, MING HO|||DA|^ |^AAAA^61616161
PV1|1|I|SUR^ICU^05||| ||||||||||| HN07000888B||| |||||||||||20070821042200
```

```
BAT|T|I|2006V1C0V02||| ||||||||||| HN03000888B||| |||||||||||S00308ST04SS00
IKT|T|CHAM^ WING HO|||DY|^ |vvvvvvv^ETETETET
PID|T||HKID:UC0001TSS~PKey:00022244||CHEUNG^LYI WING||19780101|M||CH|^W^TTT CY21GE BEYK EDV22B|||M| |||||||||||N
```

Major Download Channels

1. Downloading of patient demography / ADT
 - ◆ Patient particulars
 - ◆ Capturing events like:
 - ▶ Patient registration
 - ▶ Add / Update patient information
 - ▶ Merge patient
 - ▶ Discharge patient
2. Downloading of Allergy
3. Downloading Out-Patient Medication
4. Downloading of standardized lab result

Major Upload Channels

- 5. Uploading of APACHE data
- 6. Uploading of reports in PDF format
- 7. Uploading of ICU transfer summary data (to CMS)



Corporate level IT security

IT Security Mix

Data Security

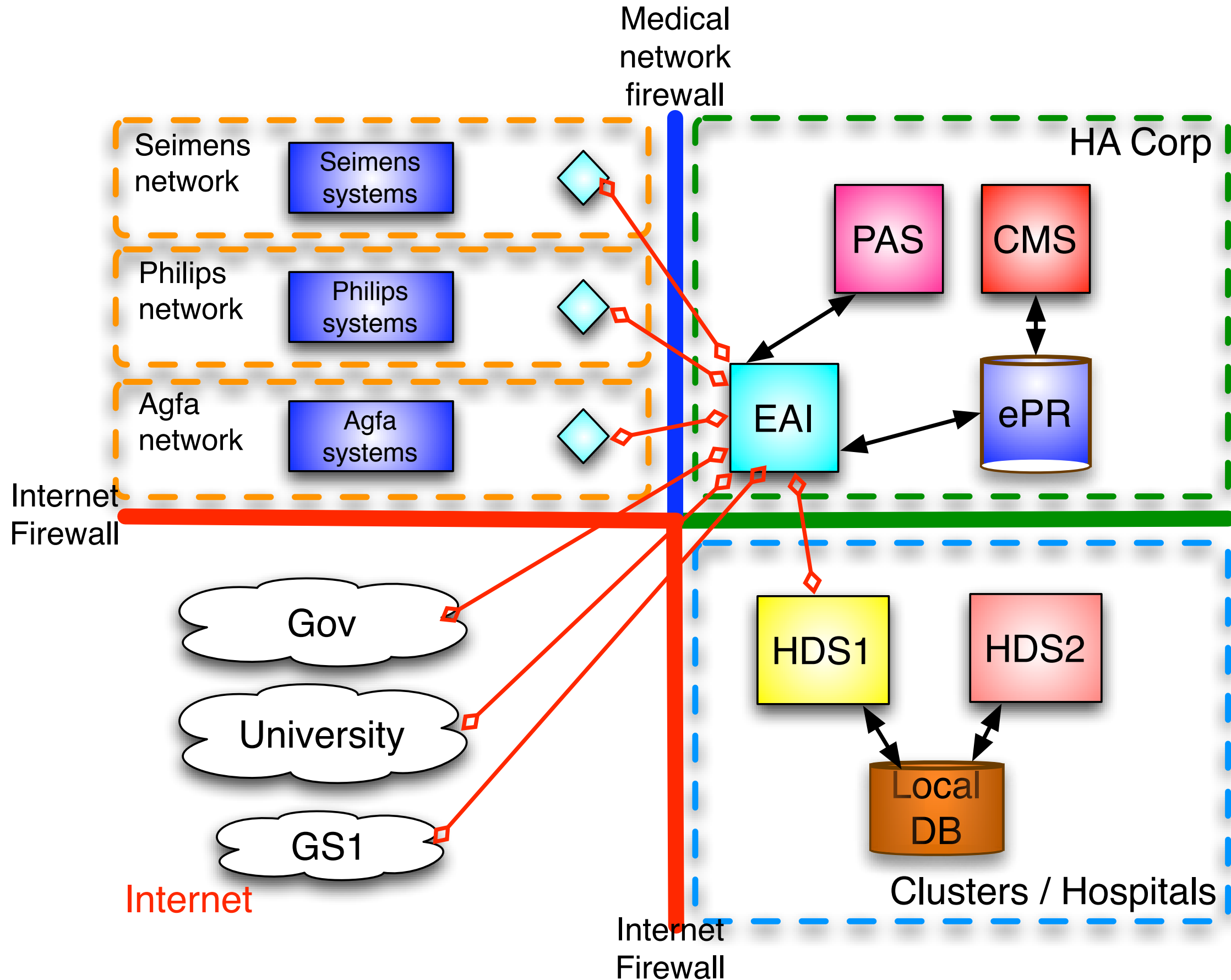
Network Security

Application Security

Server Security

- ❖ Firewall
- ❖ Anti-Virus
- ❖ Software updates
- ❖ Controlled data transmission

Coverage of Clinical Data Integration



Remote Access

Need to be “Client-less”





Challenges



Quality Assurance

♣ Data validation

♣ Workflow validation



Project Management & User Involvement

Different phases

- 1.Planning
- 2.Design
- 3.Implementation

Different roles

- 1.Clinical users / Budget holders
- 2.Administrators
- 3.Data sources
- 4.ITD integration / project teams
- 5.External vendors

	User	Adm	Data Source	ITD	Vendor
<< Planning Phase >>					
1.1. Requirement definition / project scoping	✓				
1.2. RFI / RFP	✓	✓			✓
1.3. Budget planning	✓	✓		✓	
1.4. Budget finalization	✓	✓			
1.5. Annual-Plan Target submission	✓	✓		✓	
1.6. Construct requirement spec	✓				
1.7. Sign-off requirement spec	✓				
1.8. RFQ / Tendering	✓	✓			
1.9. Project management	✓	✓			✓
1.10. Change management	✓	✓			✓
<< Design Stage >>					
2.1. System design	✓			✓	✓
2.2. Quality management	✓	✓	✓	✓	✓
2.3. Risk management	✓	✓	✓	✓	✓
2.4. Technical review			✓		
2.5. Project planning review	✓		✓	✓	✓
2.6. Sign-off functional / system spec	✓				
<< Implementation Stage >>					
3.1. Application development			✓	✓	✓
3.2. Unit testing			✓	✓	✓
3.3. Other testing (Integration test, load test, UAT)	✓		✓	✓	✓
3.4. System acceptance & sign-off	✓				
3.5. Production planning	✓			✓	✓
3.6. Post implementation review	✓	✓		✓	✓



Vendor Management

- ❖ Project scheduling
- ❖ Change request management
- ❖ Documentation, Training & Support
- ❖ Upgrade & Migration



**Get a good driver
Your CIS Administrator**



Contingency Arrangement

Thank you



James TAN
2300-7322
jamestan@ha.org.hk