Ministry of Health Malaysia

USER ACCESS CONTROL POLICY AND GUIDELINES

DISEMBER 2011

TABLES OF CONTENTS

User Access Control Policy

Policy For Control of Access to Patient Information by Users of Hospital/Clinic Information System(HIS/CIS)

Ministry of Health, Malaysia

DISEMBER 2011

A. POLICY FOR CONTROL OF ACCESS TO PATIENT INFORMATION BY USERS OF HOSPITAL/CLINIC INFORMATION SYSTEM (HIS/CIS)

1 BACKGROUND

A patient discloses information about him/herself (e.g. history) to health care providers based on the premise of patient-provider relationship.

An Electronic Medical Record (EMR) is digitally documented information about the health of an identifiable individual, recorded by a doctor or other healthcare professionals. This medical record contains history, physical examination, investigations, diagnosis, treatment and other sensitive data, that is needed to ensure continuity of care for the patient among healthcare providers.

The patient has the right to expect that there will be no disclosure of all or any of the information to persons without the patient-provider relationship unless he/she gives permission.

Therefore, there is a responsibility on the part of custodians and users of the medical record to ensure that confidentiality of medical records is maintained at all times. This is done by having a clear policy on user access control.

2 PURPOSE OF USER ACCESS CONTROL POLICY

As part of its regulatory function, the Ministry of Health makes available this policy for use by health care institutions in Malaysia for the following purposes:

i. To maintain the confidentiality of electronic patient information.

ii. Guide persons involved in the design, custody and use of clinical information systems and electronic medical records including managers of Health care facilities, health care providers both clinical and clinical support, Health IT vendors, and other users of in formulating the operational policies and procedures of user access control.
iii. As a Standard for User Access Control (UAC) for all patient data in clinical systems in the Ministry of Health (MOH), and subsequently to be adopted by other healthcare agencies and private healthcare facilities in Malaysia.

3 SCOPE AND CONTEXT OF USER ACCESS CONTROL

User access control is a procedure that forms part of Information Management. It is the mechanism for ensuring confidentiality in the context of a Computerized Clinical Information System. The major criteria for assignment of access privileges are the type of data and the means of access.

3.1 TYPE OF INFORMATION

This policy addresses information about a single patient as well as the group of patients cared for in a particular health care institution.

3.1.1 Individual patient data

The main bulk of the data is data that makes up the Electronic Medical Record (EMR). The EMR contains information pertaining to a patient`s health and illness and its management. The scope of information covered by this policy also encompasses other data regarding the patient that is obtained in order to facilitate the provision of patient care services including data regarding identity, demographics, payment methods and data required for communications. Summaries and medical reports are also individual patient data.

3.1.2 Aggregated patient data

Data of a group of patients when put together is termed as aggregated data and is also subject to user access control. These data include:

- Registries
- Extracted and analyzed clinical data
- Reports prepared for external agencies
- Prevalence and incidence of diseases
- Utilization review information e.g. Bed occupancy Rate(BOR) and length of stay (LOS)

3.2 REASONS FOR ACCESS AND MEANS OF ACCESS

In a computerized information management and communications system, care providers and other users access information regarding a patient through various applications software. Some providers may need access only to some selected parts or functions within an application-software.

The reason for access can be any or all data management processes including

- generating
- capturing
- recording
- viewing
- manipulating
- transferring
- storing
- retrieving

- analyzing
- presenting
- viewing
- copying
- printing data

These are made available as separate applications software or a comprehensive integrated system called the Hospital Information System (HIS-Fig. 1) which comprises of the following:

- Patient Management System (PMS)
- Clinical Information System (CIS)
- Clinical Support Information System (CSIS)
    - Laboratory Information System (LIS)
    - Radiology Information System (RIS)
    - Pharmacy Information System (PIS)
- Health-Information Management System(HIMS)

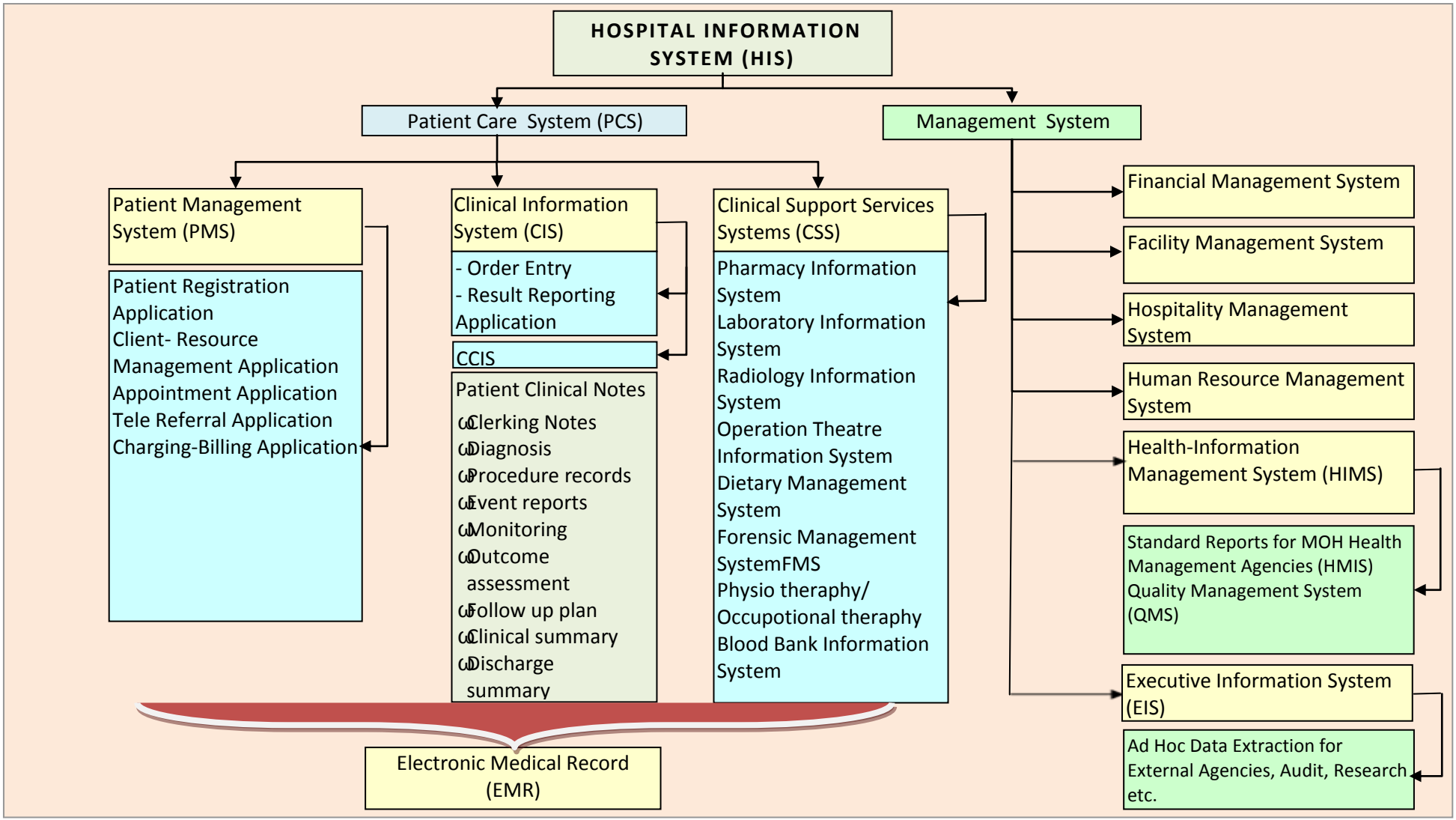


FIGURE 1: HOSPITAL INFORMATION SYSTEM

3.3 CATEGORIZATION OF USERS

Patient data is used not only by care providers but also other professionals. Users of the EMR belong to two categories i.e.

	Users	Purpose of Use
1	Primary users	Use for purposes of managing disease
2	Secondary users	Use of data of one or more patients for purposes other than managing the patient"s curre

FIGURE 2 : MAIN CATEGORY OF USERS OF PATIENT INFORMATION

4 GUIDING PRINCIPLES

The formulation of this policy is guided by the following principles

i. All rights of access to patient information originate from the expressed or implied consent given by the patient
ii. This consent is translated into patient provider relationships. The information given by the patient or gathered by the care-provider about him/her is privileged information.
iii. Access to EMR by a care provider depends on the roles or functions accorded to him or her by each healthcare facility.
iv. Care providers are bound by the Code of Ethics of their profession regarding the confidentiality of patient information.
v. All persons involved in the care of the patient and in the management of the data are responsible for the confidential
vi. The person in charge of the healthcare facility shall be responsible for putting in place the operational policies and procedures for the proper management of patient information
vii. This User Access Control policy fulfils the legal requirements of parts pertaining to it within various laws, regulations, rules and circulars including
    a. The Medical Act 1971,
    b. The Malaysian Medical Council (MMC) Ethical Codes and Guidelines:
        ¶ Code of Professional Conduct

- ¶ Duties of a Doctor
  - o Good Medical Practice
  - o Patient Confidentiality

c. Ministry of Health Circulars and Guidelines:
   - ¶ Management of Patient Medical Records in Hospitals and Medical Institutions (2010)
   - ¶ ICT Security Policy (2010)

d. Guidelines issued by other health care professional bodies

In addition to the above, the following laws apply to all healthcare facilities in the private sector:

i. Private Healthcare Facilities and Services Act 1998
ii. Personal Data Protection Act 2010

4.1 DEGREE OF CONTROL

These policies take into consideration the delicate balance between probability of loss of confidentiality and the need for availability of adequate information to ensure continuity of care.

5 OBJECTIVES OF USER ACCESS CONTROL

The basic principle for access to patient information shall be strictly on a need to know basis. This policy shall guide and facilitate user access control activities to achieve the following:

i. For authorized persons (users), access is allowed only to relevant information required to perform work
ii. Patient information is disseminated only to relevant persons or parties
iii. Prevent access to all information by unauthorized persons

6 OUTLINE OF POLICY

The policy ensures:

i. User access shall be properly managed

ii. Permission shall be granted on a need to know basis.
iii. The scope of access shall be limited by:
    a. Care Provider–Patient relationship
    b. Role or Function
    c. Location
iv. Approach to Granting Access shall take into consideration that
    a. Continuity of care is facilitated
    b. Confidentiality is safeguarded
v. Access to patient information shall be monitored and mechanisms shall be in place to prevent improper access

The relevant authorities shall ensure that the design of the HIS/CIS built or procured possesses effective access control functions and tools.

7 ELABORATION OF POLICIES

7.1 MANAGEMENT AND ADMINISTRATION OF USER ACCESS CONTROL

7.1.1 Responsibility

The overall responsibility regarding access control of clinical data belongs to the person in charge of the health care facility. He/she shall ensure that ensuring the operational policy and procedures is guided by the policy documented here.

Because control of user access to patient information is an information management function, he/she may delegate this responsibility to the Information System Manager (e.g. Chief Information Officer) or any other persons involved in managing clinical information such as the Chief Medical Record Officer or Head of Information Technology Unit. The person in charge should seek advice from individual care providers or from groups such as Medical Record Committees or Information Management Committees.

7.1.2 Execution

The person in charge shall designate suitable person(s) such as Medical Record Officers, Information Technology professionals or Clinicians where relevant to

execute the access control operational policies and procedures. Their duties shall be clearly spelt out and they shall be adequately facilitated to perform these duties.

7.1.3 Oversight

The health care facility shall ensure the effective implementation and enforcement of the User Access Control Policy.

7.2 GRANTING OF ACCESS

Determination of Limits of Access shall be determined by each healthcare facility for each individual or group of care providers based on their assigned roles, function and location.

7.3 APPROACHES, METHODS AND MECHANISMS

The health care facility shall select the most appropriate user access control methods. However, any method put in place shall have the following mechanisms:

i. Valid users shall be identified and maintained in a Register
ii. An Authorization Matrix / Security Matrix shall be constructed to allocate access to individual users and user groups.
iii. There shall be a means for identifying each individual user at every instance of access
iv. Data input tools and data views shall be customized for the individual user depending on his/her role and the provider group that he/she belongs to
v. There are mechanisms to record all instances of access whether for viewing or data entry
vi. Modification and manipulation of data may be allowed only in prescribed circumstances. It should be mandatory that reasons for such actions are documented
vii. There shall be an Audit Trail detailing the person, date, time and circumstance when the information system or data is accessed
viii. Methods and mechanisms shall be put in place to discourage, prevent and monitor unauthorized access or disclosure of patient information. This should include some form of disciplinary action

Computerized information systems shall utilize security management tools for user access control procedures. It is the responsibility of the health care facility to ensure that the EMR applications built or procured has proper access control tools in place and relevant staff members are trained to use them.

7.4 EXCEPTIONS

i. „Breaking glass" policy for care provider in emergency "live threatening situations". reason of access. Alert will be sent to director of facility. The access to patient information by authorised health care providers is logged.
ii. The patient himself can have access to his medical information subject to the procedures determined by the custodian of information; except in cases where the information is deemed detrimental to his physical or mental health.
iii. The patient"s appointed representative o access to all medical information or data on order by court of law.
iv. Data may be disclosed e.g. when the government by statute/legislation requires information for the public good in cases of epidemics and notifiable diseases.

7.5 GRADES OF CONFIDENTIALITY OF DATA

Due consideration shall be given to the degree of confidentiality of medical information and certain additional precautions may be taken to safeguard their confidentiality. The following are considered as **highly confidential data**:

i. Data of medico-legal cases (murder, rape, assault, child abuse, drug abuse, litigation against a care provider or the institution)
ii. Data of patients with certain diseases e.g. STD, Psychiatric conditions, HIV infection and AIDS
iii. Data of persons which might be of public interest.
iv. Data of patients if known to others may cause embarrassment or harm to him/her e.g. adoption records

7.6 SECONDARY USE OF MEDICAL RECORD

i. Use of patient data, for purposes other than immediate patient care, is also subject to user control policy.
ii. IT professionals and medical record officers involved in performing data extraction shall be given access to the EMR with cautions and restrictions spelt out.
iii. Extracted data in the form of summaries e.g. medical reports shall be given only to appropriate parties and always with the expressed consent of the patient.
iv. Discharge summaries used in referrals are given to other care practitioners if the patient has agreed to seek treatment or services from the providers being consulted or referred to.
v. Data for audits, quality management and HMIS shall as far as possible be depersonalized
vi. For research purposes, what patient information can be accessed shall be determined by the relevant department heads as well as the facility research ethical committee and the Medical Research Ethics Committee (MREC)at MOH, where needed.
vii. Access to a patient" s information by a st or training is subject to approval from the custodian of the information.

8 CONCLUSION

Thus, in summary, the effective adoption, implementation and enforcement of this User Access Control Policy will ensure that all electronic patient information shall remain confidential. To this end, all HIS/CIS facilities shall institute adequate measures to:

i. Protect patient information from unauthorized access
ii. Have a multilayered approach utilizing multiple access point safeguards
iii. Streamline user authorization and secure access across facilities
iv. Track users throughout the facility for a complete activity snapshot
v. Have a centralized monitoring, control and assignment of access levels for simplified IT management at the facility.

User Access Control Policy

GUIDELINES FOR THE IMPLEMENTATION OF USER ACCESS CONTROL POLICY

(To be customized according to the needs of individual facilities)

Ministry of Health, Malaysia

DISEMBER 2011

B.GUIDELINES FOR THE IMPLEMENTATION OF USER ACCESS CONTROL POLICY

1 INTRODUCTION

An Electronic Medical Record (EMR) is digitally documented information about the health of an identifiable individual, recorded by a doctor or other healthcare professionals. The patient has the right to expect that there will be no disclosure of all or any of the information to persons without the patient-provider relationship unless he/she gives permission. Therefore, there is a responsibility on the part of custodians and users of the medical record to ensure that confidentiality of medical records is maintained at all times. This is done by having a clear User Access Control Matrix.

It is the intent of this document to guide persons involved in, the design, custody and use of clinical information systems and electronic medical records, including managers of health care facilities, health care providers both clinical and clinical support, health IT vendors, and other users, in constructing the User Access Control Matrix of their respective healthcare facilities.

2 OBJECTIVES

2.1 GENERAL OBJECTIVES

To ensure that the confidentiality of electronic patient information is maintained as required by the law.

2.2 SPECIFIC OBJECTIVES

2.2.1 The basic principle for access to patient information shall be strictly on a need to know basis.

2.2.2 For authorized use access is allowed only to relevant information required to perform work

2.2.3 Patient information is disseminated only to relevant persons or parties

2.2.4 Prevent access to all information by unauthorized persons

3 HOW TO USE THESE GUIDELINES

This document aims to help every facility come out with its own customized matrix that fulfils that facility"s user access con and location.

The User Access Control Policy is the parent document to this and as such should be used along with these guidelines.

4 USER ACCESS CONTROL MATRIX

4.1 USER ACCESS ROLE DEFINITION

4.1.1 **Patient Care** – a role of managing a particular illness which is related to the patient.

4.1.2 **Administration** – managing the work process or flow in the particular department or unit.

4.1.3 **Audit & Research** – Monitoring services by tabulating statistics and producing reports that is related to the particular department under their care. Gathering information for research purposes.

4.1.4 **Education** – Learning activity using the patients" i

4.1.5 **Epidemiology** – Is the study of the occurrence, distribution and determinants of states of health and disease in human groups and populations and the application of this study to the control of health problems.

4.1.6 **Register** – Is a record in writing as a verb; it is to record or to be recorded in an official list.

4.2 OPTIONS IN STANDARD OPERATING ENVIRONMENT

4.2.1 Read

4.2.2 Write

4.2.3 Print – All users are not allowed to print unless granted by custodian of information.

4.2.4 No access

4.2.5 Not applicable

4.3 USER ACCESS MATRIX

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation	
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
A.	Doctors											
	a. Hospital Director											
	¶ Admin	1.	Read	Read	Read	Read	Read	Read	Read	Read	Access to all patient data within his facility.	No exceptions
	¶ Audit & Research	2.	Read	Read	Read	Read	Read	Read	Read	No Access	Access to all patient data within his facility.	No exceptions
	¶ Patient Care	3.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	Read	No Access	Access to all patient data within his facility if he is treating the patient	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	b. Head of Department											
	¶ Admin	4.	Read	Read	Read	Read	Read	Read	No Access	No Access (except – full paying patient)	Access to all patient data within his department only.	In the absence of a Hospital Director, a designated H.O.D. has the access to all patient data within the facility.
	¶ Audit & Research	5.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.
	¶ Patient Care	6.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to all patient data within his department	Override allowed in referred and emergency cases.
	¶ Education	7.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
	c. Specialist												
	¶ Admin	8.	Read	Read	Read	Read	Read	Read	No Access	No Access (except – full paying patient)	Access to all patient data within his department only.	In the absence of H.O.D., a designated Specialist has the access to all patient data within the department.
	¶ Audit & Research	9.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.
	¶ Patient Care	10.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to patient data under his care	Override access under: -Emergency (Break the glass)
	¶ Education	11.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to patient data	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	d. Family Medicine Specialist											
	¶ Education	12.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to patient data under his care.	No exceptions
	¶ Audit & Research	13.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.
	¶ Patient Care	14.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to patient under his care.	Override access under: 1) Emergency 2) Referral
	¶ Admin	15.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to patient data under his care.	No Exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	e. Medical / Dental Officer											
	¶ Hospital with specialists											
	¶ Audit & Research	16.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.
	¶ Education	17.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to patient data under his care.	No exceptions
	¶ Patient Care	18.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to patient data under his care.	Override access under: 1) On call 2) Emergency 3) Referral
	¶ Hospital without specialist											

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Audit & Research	19.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.
	¶ Education	20.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to patient data under his care.	No exceptions
	¶ Patient Care	21.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to patient data under his care.	Override access under: 1)On call 2) Emergency 3) Referral
	¶ Health Care Facilities											
	¶ Audit & Research	22.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Education	23.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to patient data under his care.	No exceptions
	¶ Patient Care	24.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to patient data under his care.	Override access under: 1) On call 2) Emergency 3) Referral
	¶ Admin	25.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his facility only	No exceptions
	f. House Officer											
	¶ Audit & Research	26.	Read	Read	Read	Read	Read	Read	No Access	No Access	Access to all patient data within his department only.	Access to all referred cases to his specialty.
	¶ Education	27.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Access to patient data under his care.	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Patient Care	28.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Access to patient data under his care.	Override access under: 1) On call 2) Emergency (No role to accept referral)
B.	Nurses											
	i) Hospital setting											
	a. Matron / sister											
	¶ Admin	29.	Read	Read	Read	Read	Read	Read	No Access	No Access	Only for patient under their area / department / facility	No exceptions
	¶ Audit & Research	30.	Read (MRN and name only)	No Access	No Access	Read	Read	Read	No Access	No Access	Only for patient under their area / department / facility.	Override allowed for external auditing.
	¶ Education	31.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Only for patient under their area / department / facility	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Patient Care	32.	Read	Read	Read	Read	Read	Read	No Access	No Access	1) Only for patient under their area / department / facility. 2) Can read & write only during emergencies. Only can access on nursing notes.	Override allowed during on-call.
	b. Staff Nurse											
	¶ Education	33.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Only for patient under their area / department / facility	No exceptions
	¶ Audit & Research	34.	Read	No Access	No Access	Read	Read	Read	No Access	No Access	Only for patient under their area / department / facility.	Override allowed for external auditing.

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Patient Care	35.	Read & Write	Read & Write	Read & Write	Read & Write	Read & Write	Read & Write	No Access	Read & Write (to charge / itemize for FPP patients)	a) Only for patient under their area / department / facility. b) Only can write on nursing notes	No exceptions
	¶ Registration	36.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Not Applicable	Register role Only in the absence of the registration clerks.	No exceptions
	c. Community Nurse											
	¶ Patient Care	37.	Read	Read	Read	Read	Read	Read	No Access	No Access	Only can write on nursing notes	No exceptions
	¶ Registration	38.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	No Access	Register role Only in the absence of the registration clerks.	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
	d. Dental Nurse												
	¶ Patient Care	39.	Read	Read	Read & Write	Read & Write	Read	Read & Write	No Access	No Access	Only can write on dental notes		No exceptions
	¶ Audit Research & Education	40.	Read	Read	Read	Read	Read	Read	Read	Read	Only for patient under their area		No exceptions
	e. Dental Surgery Assistant												
	¶ Patient Care	41.	Read	Read	Read	Not Applicable	Not Applicable	Not Applicable	No Access	No Access			No exceptions
	¶ Registration	42.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Read & Write**	Only in the absence of the registration clerks. ** In the absence of billing Unit.		

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	ii) Health Care Facilities											
	a. Matron / Sister											
	¶ Admin	43.	Read	Read	Read	Read	Read	Read	Read	Read	Only for patient under their area / facility.	Override allowed if there is no matron in the area.
	¶ Patient Care	44.	Read	Read	Read	Read	Read	Read	No Access	No Access	1) Only for patient under their area / department / facility. 2) Only during emergencies. 3) Only can write on nursing notes	Override allowed during on-call.
	¶ Audit, Research & Education	45.	Read	Read	Read	Read	Read	Read	Read	Read	1) Only for patient under their area. 2) Only on nursing care.	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
	b. Staff Nurse												
	¶ Patient Care	46.	Read	Read	Read	Read & Write	Read & Write	Read & Write	No Access	No Access	Only for patient under their area / facility. Only can write on nursing notes	No exceptions	
	¶ Audit, Research & Education	47.	Read	Read	Read	Read	Read	Read	Read	Read	1) Only for patient under their area. 2) Only on nursing care.	No exceptions	
	¶ Registration	48.	Read & Write	Read & Write	Not applicable	Not applicable	Not applicable	Not applicable	Read & Write	No Access	Register role Only in the absence of the registration clerk.	No exceptions	
	c. Community Nurse												
	¶ Education	49.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Only for patient under their area / department / facility	No exceptions	

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
	¶ Registration	50.	Read & Write	Read & Write	Not applicable	Not applicable	Not applicable	Not applicable	Read & Write	No Access	Role as Only in the absence of the registration clerks.		No exceptions
	¶ Patient Care	51.	Read	Read	Read & Write	Read & Write	Read	Read & Write	No Access	No Access	Only in the absence of the staff nurses Only can write on nursing notes		No exceptions
	d. Dental Nurse												
	¶ Patient Care	52.	Read	Read	Read & Write	Read & Write	Read	Read & Write	No Access	No Access	Only can write on dental notes		No exceptions
	¶ Registration	53.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	No Access	Only in the absence of the registration clerk		No exceptions
	¶ Audit, Research & Education	54.	Read	Read	Read	Read	Read	Read	Read	Read	Only for patient under their area.		No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	e. Dental Surgery Assistant											
	¶ Patient Care	55.	Read	Read	Read	Not Applicable	Not Applicable	Not Applicable	No Access	No Access		No exception
	¶ Registration	56.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Read & Write**	Only in the absence of the registration clerks. ** In the absence of billing Unit.	
	iii) Health Care Facilities											
	a. Matron											
	¶ Admin	57.	Read	Read	Read	Read	Read	Read	Read	Read	Only for patient under their area / facility.	Override allowed if there is no matron in the area.
	¶ Audit	58.	Read	Read	Read	Read	Read	Read	Read	Read	1) Only for patient under their area. 2) Only on nursing care.	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	b. Sister											
	¶ Admin	59.	Read	Read	Read	Read	Read	Read	Read	Read	Only for patient under their area / facility.	Override allowed if there is no sister in the facility.
	¶ Audit	60.	Read	Read	Read	Read	Read	Read	No Access	No Access	Only for patient under their area / facility.	No exceptions
	c. Staff Nurse											
	¶ Patient Care	61.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only for patient under their area / facility. Only can write on nursing notes	No exceptions
	¶ Registration	62.	Read & Write	Read & Write	Not applicable	Not applicable	Not applicable	Not applicable	Read & Write	No Access	Only in the absence of the registration clerk.	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
	d. Community Nurse												
	¶ Patient Care	63.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on nursing notes		No exceptions
	¶ Registration	64.	Read & Write	Read & Write	Not applicable	Not applicable	Not applicable	Not applicable	Read & Write	No Access	Only in the absence of the registration clerks.		No exceptions
	e. Asst. Nurse												
	¶ Patient Care	65.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on nursing notes		No exceptions
	¶ Registration	66.	Read & Write	Read & Write	Not applicable	Not applicable	Not applicable	Not applicable	Read & Write	No Access	Only in the absence of the registration clerks.		No exceptions
	f. Midwifes												
	¶ Patient Care	67.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on nursing notes		No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Registration	68.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	No Access	Only in the absence of the registration clerks.	No exceptions
	g. Dental Nurse											
	¶ Patient Care	69.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on nursing notes	No exceptions
	¶ Registration	70.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Read & Write	Only in the absence of the registration clerks.	
	h. Dental Surgery Assistant											
	¶ Patient Care	71.	Read	Read	Read & Write	Not Applicable	Not Applicable	Not Applicable	No Access	No Access		No exceptions
	¶ Registration	72.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Read & Write**	Only in the absence of the registration clerks. **In the absence of billing Unit	

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
C.	Medical Assistant												
	i) Hospital Setting												
	¶ Patient Care	73.	Read & Write	Read & Write*	Read & Write	Read & Write	Read & Write*	Read & Write	No Access	No Access	Read & Write in: 1) A & E 2) Designated specialist clinic		No exceptions
	¶ Registration	74.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Read & Write	Only in the absence of the registration clerks. Only can write on nursing notes		No exceptions
	ii) Health Care Facilities												
	¶ Patient Care	75.	Read	Read	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access			No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation		
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills			
	¶ Registration	76.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Read & Write	Read & Write	Only in the absence of the registration clerks.		No exceptions
D.	Healthcare Assistants												
	¶ Patient Care	77.	No Access	No Access	No Access	No Access	No Access	Not Applicable	No Access	No Access	Not Applicable		No exceptions
	¶ Registration	78.	Read & Write	Read & Write	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Only in the absence of the registration clerks.		No exceptions
E.	Pharmacists												
	¶ Admin	79.	Read	No Access	No Access	No Access	Read	Read (med. only)/ TDM	No Access	No Access			No exceptions
	¶ Audit	80.	Read	No Access	Read	No Access	Read	Read	No Access	No Access			No exceptions
	¶ Dispensing	81.	Read	Read	Read	Read	Read	Read & Write *	No Access	Read	Write* dispensing notes		No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
	¶ Patient Care	82.	Read	Read	Read	Read	Read	Read & Write	No Access	Read	Write* Pharmacist Notes	No exceptions
F.	Assistant Pharmacists											
	¶ Dispensing	83.	Read	No Access	No Access	No Access	Read	Read * & Write *	No Access	No Access	Read* prescription pharmacist notes Write* dispensing notes	No exceptions
G.	Medical Lab Technicians											
	¶ Perform Lab Orders	84.	Read & write	No Access	No Access	No Access	Read	Read & Write* (results of Ix.)	No Access	No Access	Amendment & addendums*	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
H.	Dental Lab Technologist / Prosthetic & Orthotics Technician											
	¶ Fabrication of Prosthetics / Orthotics	85.	Read	No Access	No Access	No Access	Read	Read	No Access	No Access		
I.	Optometrists											
	¶ Patient Care	86.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on optometrist notes	No exceptions
J.	Audio-metrists											
	¶ Patient Care	87.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on audiometrist notes	No exceptions
K.	Therapists											
	a. Occupational											
	¶ Patient Care	88.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on therapist	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
											notes	
	b. Speech											
	¶ Patient Care	89.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on therapist notes	No exceptions
	c. Physio											
	¶ Patient Care	90.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on therapist notes	No exceptions
	d. Clinical Psychologist											
	¶ Patient Care	91.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on therapist notes	No exceptions
	e. Prothetist & Orthotists											
	¶ Patient Care	92.	Read	No Access	Read & Write	Read & Write	Read & Write	Read & Write	No Access	No Access	Only can write on therapist notes	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
L.	Dietician / Nutritionists											
	¶ Patient Care	93.	Read	No Access	Read	Read	Read	Read & Write	No Access	No Access	Only can write on dietician notes	No exceptions
M.	Radiographer	94.	Read	No Access	No Access	No Access	Read	Read#,	No Access	No Access	#Only Radiology Ix	No exceptions
N.	Health Education Officer											
	¶ Health Promotions	95.	Read	No Access	Read	No Access	Read	No Access	No Access	No Access		No exceptions
O.	Assistant Environmental Health Officer											
	¶ Control of notifiable disease	96.	Read	No Access	Read	Read	Read	Read & Print	No Access	No Access		No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
P.	Medical Record Officer											
	¶ Admin	97.	Read	Read	Read	Read	Read & Write (ICD coding)	Read	Read	Read		No exceptions
	¶ Audit & Research	98.	Read	Read	Read	Read	Read	Read	No access	Read		Only can print statistical report
Q.	Medical / Dental / Undergraduate											
	¶ Patient Care	99.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access		Accessibility should be through HOD with restricted period/ only
	¶ Education Training	100.	Read	No Access	Read	Read	Read	Read	No Access	No Access		Accessibility should be through HOD with restricted period/ only Patient that refused need to be blocked

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									Exceptions
			Demographic Data		Clinical Data				Financial Data		Explanation	
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
R.	Lecturers / Tutors / Preceptors											
	¶ Education	101.	Read	No Access	Read	Read	Read	Read	No Access	No Access	During the contract period only	No exceptions
S.	Researcher											
	¶ Research & Planning	102.	Read	Read	Read	Read	Read	Read	No Access	No Access		No exceptions
	¶ Epidemiology	103.	Read	No Access	Read	Read	Read	Read	No Access	No Access		No exceptions
	¶ Clinical Research	104.	Read	No Access	Read	Read	Read	Read	No Access	No Access	Modifiable for particular protocol study & during study period only	
T.	Non-Clinical Administrator											
	¶ Admin	105.	Read	No Access	No Access	No Access	No Access	No Access	Read	Read		No exceptions
	¶ Audit	106.	Read	No Access	No Access	No Access	No Access	No Access	Read	Read		No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
U.	Medical Social Worker											
	¶ Evaluate financial status and provide assistance for the needy.	107.	Read	Read	Read	No Access	Read	Read	Read	Read		No exceptions
V.	System Administrator	108.	Read	No Access	No Access	No Access	Read	No Access	No Access	No Access		No exceptions
	¶ System Administrator (Operational)	109.	Read	Read	Read	Read	Read	Read	Read	Read	Addendum when requested with documentation	For trouble shooting & must be documented
W.	Patient	110.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access		No exceptions Print report through Medical Records
X.	Appointed rep. / legal guardian (upon consent)	111.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access		No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment									
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
Y.	Courts											
	¶ Negligence / Suits	112.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access		No exceptions Print of medical record on court request
Z.	Insurance Companies (upon consent)	113.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access		No exceptions Print of medical record on patient request
AA.	Employers	114.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access		No exceptions
BB.	Allied Health Profession Students	115.	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	Under the direct supervision of their tutor of trainer. Only for particular discipline	No exceptions

No.	Area of accessibility / User Roles	Row	Standard Operating Environment										
			Demographic Data		Clinical Data				Financial Data		Explanation	Exceptions
			Person Identification Data	Next of Kin	History	Physical	Diagnosis	Ix / Mx	Salary	Bills		
CC.	Counseling Officers											
	¶ Patient Care	116.	Read	Read	Read & write	Read	Read & write	Read & Write*,	No Access	No Access	Only can write on counselor notes	No exceptions

User Access Control Policy

TECHNICAL REQUIREMENTS FOR USER ACCESS CONTROL AT HOSPITAL / CLINIC INFORMATION SYSTEM (HIS/CIS)

(To be customized according to the needs of individual facilities)

Ministry of Health, Malaysia

DISEMBER 2011

C. TECHNICAL REQUIREMENTS FOR USER ACCESS CONTROL AT HOSPITAL / CLINIC INFORMATION SYSTEM (HIS/CIS)

1 INTRODUCTION

In any access control model, the entities that can perform actions in the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects

2 ACCESS CONTROL SYSTEM

2.1 IDENTIFICATION AND AUTHENTICATION (I&A)[1]

2.1.1 Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that makes an assertion or claim of identity. The I&A process assumes that there was an initial validation of the identity, commonly called identity proofing.

2.1.2 Authenticators are commonly based on at least one of the following four factors:

- ¶ Something you know, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- ¶ Something you have, such as a smart card or security token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- ¶ Something you are, such as fingerprint, voice, retina, or iris characteristics.
- ¶ Where you are, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.

2.2 AUTHORIZATION

2.2.1 Authorization applies to subjects. Authorization determines what a subject can do In the system.

2.3 ACCOUNTABILITY

2.3.1 Accountability uses such system components as audit trails (records) and logs to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- ¶ Detecting security violations
- ¶ Re-creating security incidents
- ¶ Detering future security violations.

3 ACCESS CONTROL MODELS

Access control models categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC and RBAC are both non-discretionary. MOH REQUIREMENT IS BASED ON RBAC MODELS.

4 ROLE BASED ACCESS CONTROL (RBAC) [2,3,]

Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permission to perform particular system functions.

4.1 THREE PRIMARY RULES ARE DEFINED FOR RBAC:

4.1.1 Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a role.

4.1.2 Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

4.1.3 Transaction authorization: A subject can execute a transaction only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

4.1.4 Constraints are restrictions that are enforced upon access permissions. They can include contextual properties such as separation of duties, time-dependency, mutual exclusivity, cardinality, or location, etc. Constraints may be enterprise specific. Examples of permission constraints could include:

i. Head Nurse permission functions can be accessed only by one Registered Nurse per 12-hour shift on a hospital floor at any given time (cardinality of 1, time-dependency),

ii. Only one Physician may have access to the Chief of Staff permission (cardinality of 1),

iii. A laboratory user can co-sign another Lab Technician"s co-sign their own even if logged on as the Lab Technician Supervisor (separation of duties),

iv. Provider"s access to a remote hospital th (location), and

v. A physician working scheduled clinic hours (time-dependency) vs. physician working in a 24 hour Emergency Room (no time-dependency).

5 FUNCTIONAL REQUIREMENT STATEMENT OF USER ACCESS CONTROL

5.1 PRE-ACCESS

5.1.1 Right Person

i. **Right User**

a. Every user must key-in his/her User ID, Password

b. Biometrics can be used to recognize a valid user

c. Key-in category and discipline/department.(To construct Job Matrix/Security matrix that block by discipline)

d. Declaration of relationship (Patient-care provider)

e. Health care provider must be on duty (To develop Electronic Rostering module / function)

ii. **Right Patient**

a. Patient needs to register at facility

b. Biometrics can be used to recognize a valid patient

c. Assigned or classified to specific discipline/department/team or specific health care provider

5.1.2 **Right time**

i. **Active Record and In-Active Record**

a. Active Record – Once patient register at facility

b. In- Active record (closed record) – After patient is discharged from the facility there must be a time period be closed. (e.g. Inpatient: After 3 months from date of discharge, Outpatient: After 1 month from date of discharge per encounter)

c. To access the encounter record after 3 months:

¶ Patient must register again at healthcare facility

¶ On request (must follow procedure to trace patient record)

ii. User must be on duty to have access.

a. To develop electronic rostering function/module

5.1.3 **Right Location**

i. Patient record only can be accessed within the MOH network or facility network.

ii. User can only have access at their dedicated place of work or location

iii. Table below shows how access is given according to location.

NO	ACCESS TYPE	ACCESS	USER
1.	LOCATION	¶ Only at that location ¶ Inpatient / Outpatient ¶ Clinic / Ward ¶ Discipline: e.g.O&G. A&E etc	HO, SN, AN, MS, JM, SISTER, Allied Services
2.	ROLE DEFINED	1 Referral 2 Audit 3 Education 4 Administration Access can be made from location within the healthcare facility	Consultant /Specialist/ HOD, Matron, MO

5.1.4 **Right Function and Activity**

i. To develop Menu or Sub Menu Matrix

ii. For each data segment and the corresponding applications software functionality, the users/user groups will be allowed to perform any one or all of the following data management functions **(refer to Appendix B)**:

a. Generate, and record the data (write) as part of their work

b. Retrieve, View and use the data (Read) as part of their work

c. Manipulate (Modify, correct, delete) the data

5.1.5 **Right Info**

i. Different User Interface for Different User (segmentation of data)

ii. For each user, the data segments and the corresponding applications software functionality that he/she will be allowed to use while performing his/her work is identified. **(refer to Appendix C; Figure 2 & 3)**

iii. To develop a notes/reports an assignment matrix

5.1.6 **Security for Highly Confidential Data (HCD)**

i. Remove: All existing access by applying „block"

ii. Assign: Specific Authorized Care Providers or group of care providers

5.2 DURING ACCESS

5.2.1 **Warning Statement**

i. Basic warning (Layer 1): General Alert

ii. Second warning (Layer 2): Category/Job Matrix/Location

iii. Third warning (Layer 3): Access Denied/Lock (Enter Special Code)*For highly confidential data. (red flag by Director or committee)

5.2.2 **Break Glass/Code Blue**

i. Break glass code

ii. Alert to facility director or responsible person depending on the facilit Information Security Policy

iii. Logged

5.3 POST-ACCESS

5.3.1 **Audit Trail**

i. Audit Trail Capture:
   a. Time/ Date/ Location Access
   b. User_Id
   c. Create, View, Update, End of Module and Functions Used
   d. Hit Counter/Statistic

ii. Dedicated module for audit trail

iii. Schedule and Ad-hoc

iv. Monitoring Person (Pengarah/Head of IT

Appendix

Ministry of Health, Malaysia

DISEMBER 2011

APPENDIX A - GENERIC OF USER ACCESS CONTROL

1.1 HOSPITAL PUTRAJAYA

NO	ACCESS TYPE	ACCESS	USER
1.	LOCATION	• Only at that location • Inpatient / Outpatient • Clinic / Ward	HO, SN, AN, MS, JM, SISTER, Allied Services
2.	ROLE DEFINED	1. Referral 2. Audit 3. Education 4. Administration Access can be made from anywhere within the healthcare facility	Consultant Specialist / HOD, Matron, MO
3.	HIGHLY CONFIDENTIAL	• Data Blocked • Allowance of access by referring Doctors • This must be role defined Access can be made from anywhere within the healthcare facility	• Consultant Specialist • Inpatient: as long as in ward • Outpatient: once sent home • Idle for 1 hour or 5 pm

NO	ACCESS TYPE	ACCESS	USER
4.	SPECIALITY	Upon discharge: Only allow user to read according to their speciality. If they want to access other than their speciality they have to be role defined. This applies only to Medical Officer and Specialist. Nursing Staff, Allied Health Staff, Houseman and students will have no exception- however if they need to, they can go to Medical Records Office. If they want to access other than their speciality they have to be role defined.	

- For inpatient, if the patient is referred to allied services, allied services personnel will use the referral document to give appropriately care.
- Authorization to desensitize the highly sensitive data is only made by Hospital Director
- For Medical Lab Technicians (MLT) and Radiographers, access to clinical notes is not necessary- they just need to look at the order request note

1.2 HOSPITAL SELAYANG – DYNAMIC USER

GLOSSARY OF TERMS

HO	-	House Officer
PPP	-	Penolong Pegawai Perubatan
PPK	-	Pembantu Perawatan Kesihatan
SN	-	Staff Nurse
JM	-	Jururawat Masyarakat
OSCC	-	One Stop Crisis Centre
SCAN	-	Suspected Child Abuse & Neglect

1.2.1 OUTPATIENT – WORKFLOW IN OUTPATIENT DEPARTMENT

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
1.	Scheduling & registration	Primary provider	<u>New case:</u> Referral to specific Doctor Assign privileges to referred Doctor	√	
			<u>Referral to discipline(Specialist in charge/Doctor in charge)</u> Assign to Doctor on duty at appointment date and place. May be based on expertise of care providers		√
			<u>Follow up case</u> Assign privilege to the care provider according to follow up plan	√	
		General purpose care provider (HO, nurses, PPP, JM, PPK)	Care providers where the patient will be registered are automatically given access.		√
		Pre consultation / triage – SN / optometrist / audiologist	Given access as general purpose provider.		√
2.	Carry out procedures-	Care provider providing treatment	Based on orders Person assign perform task are given access To use work list for this purpose.		

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
3.	Treatment	Care provider providing treatment i.e. pharmacist	Drug treatment- if prescription made, the pharmacist shall get access Access can be narrowed down to pharmacist of that particular dispensary or open to all pharmacists.		√
4.	Follow up	Relationship terminated	All access closed upon discharge BUT exception to certain discipline where task not completed yet for example Pathologist, Radiologist. Appointment must be given to appropriate clinic. Patient should be assigned to the same Primary provider (depending on type of cases) who is looking after the patient.	-	-

1.2.2 EMERGENCY DEPARTMENT – WORKFLOW IN EMERGENCY DEPARTMENT

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
1.	Pre-hospital care	Care provider providing treatment i.e. PPP	Person sent out with ambulance according to roster (transcribe later)	√	
2.	Triage	Care provider providing treatment i.e. PPP	Performing assessment according to roster (transcribe later)		
3.	Registration	Doctor providing care	Access open to all Doctors on duty		√

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
		General purpose staff (i.e. SN/PPP/PPK)	according to zone based on triage category (red/yellow/green/white staff)		√
4.	Assessment and treatment	Doctor providing care	Access open to all Doctors on duty		√
		General purpose staff (i.e. SN/PPP/PPK)	according to zone based on triage category (red/yellow/green/white staff)		√
		Locum Doctor providing care	Included as Doctors on duty Must be given privilege as ED Doctor if they are coming from other departments		
5.	Patient with sensitive data	Appointed Team member OSCC – SCAN team	Team members on duty	√	
6.	Referral to other specialities	Referred Doctor and team	Doctor / Team members on duty	√	

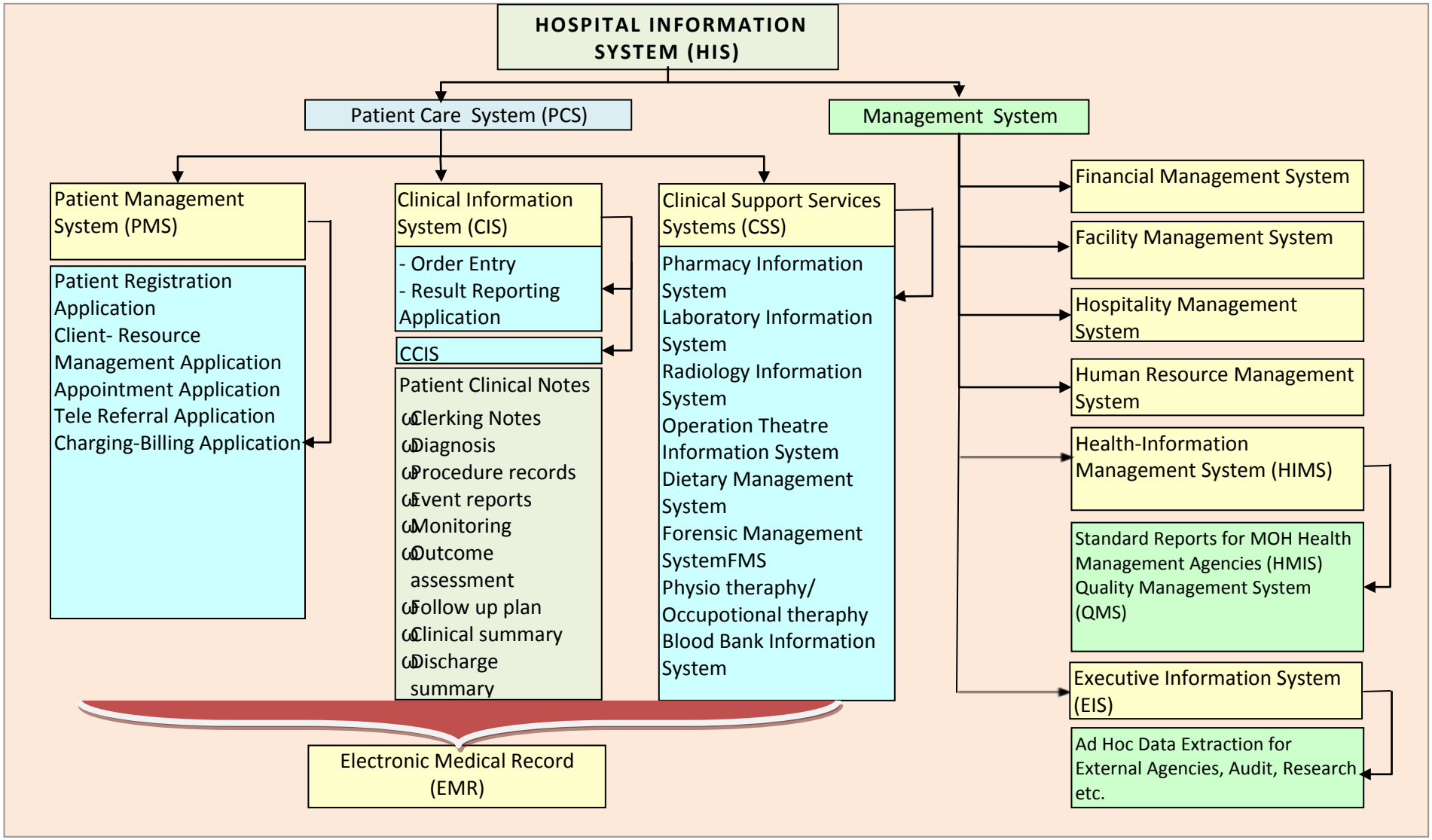
1.2.3 IN PATIENT – WORKFLOW IN WARD

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
1.	Admission:	Admitting Doctor	Shall be identified through admission form.	√	
		Primary provider	can be identified through admission form based on Doctor who look after the patient at the clinic or ED or previous admission	√	

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
		General purpose care provider (HO, nurses, PPP, JM, PPK)	Where the patient will be admitted is automatically given access.		√
		Care provider who performs clerking /assessment:	Automatic privileges shall be given to care provider according to duty roster	√	
2.	Diagnosis made:	Care team	Care plan can be triggered where the care provider performing required task are identified and Automatic privileges shall be given. (e.g. inclusion in their work list)		√
3.	Procedures/Investigations/monitoring:	Care provider performing test , examinations etc.	Accesses are given through orders. Automatically closed access once task completed.		√
4.	Referral	Co-opted care provider	Access given to the care provider to whom the case is referred.	√	
5.	Treatment:	Assigned or Co-opted care provider	Access will be given through orders.		√
6.	Transfer Location;	Additional or changed care provider (Doctor)	Current care providers retains access	√	
		General purpose care provider E.g. nurses / HO / PPK	Access of General purpose care provider of previous location is taken away and access will be given to care providers at new location.		√
7.	Transfer Specialty / department;	changed care provider (Doctor)	Provide access to specialty taking over the case		√

No.	Encounter / Task	Patient Provider Relationship	Mechanism	Assign to	
				Named Care Provider	Provider group
			Access for referring specialty can be retained or taken away depending on whether care by them need continue.		
8.	Follow-up plan		All access shall be closed upon discharge Primary care provider (depending on type of cases) who looks after the patient on follow-up must be identified. The location/clinic must be identified before discharge	-	-

APPENDIX B ï HIS FUNCTION



APPENDIX C - PRIVILEGE MATRIX FOR USERS OF CLINICAL ADMINISTRATION APPLICATION

This matrix looks at the needs from a user"s point of view.

FIGURE 1: PRIVILEGE MATRIX FOR USERS OF CLINICAL ADMINISTRATION APPLICATION (EXAMPLE)

User Category	Application	Read / View	Order	Perform Task & Enter data
Main Registration & Billing Clerk	Client Registration (PMI)	Yes	No	Yes
	Visit registration	Yes	Yes	Yes
	Billing	Yes	Print-Reprint	Yes
	Outpatient scheduling	Yes	Yes	Yes
	Inpatient ADT	Yes	No	No
Clinic Receptionist	Client Registration	Yes	No	No
	Visit registration	Yes	Yes	Yes
	Billing	Yes	No	No
	Outpatient scheduling	Yes	No	Yes
	Inpatient ADT	Yes	Yes	No
Clinic Manager / Clinic Nurse	Client Registration	Yes	No	No
	Visit registration	Yes	Yes	Yes
	Billing	Yes	No	No

User Category	Application	Read / View	Order	Perform Task & Enter data
	Outpatient scheduling	Yes	No	No
	Inpatient ADT	Yes	Yes	No
Admission clerk	Client Registration	Yes	Yes	Yes
	Visit registration	Yes	Yes	Yes
	Billing	Yes	Print-Reprint	Yes
	Outpatient scheduling	Yes	No	No
	Inpatient ADT	Yes	No	Yes
Ward clerk	Clinic Registration	Yes	No	No
	Billing	Yes	No	No
	Outpatient scheduling	Yes	Yes	Yes
	Inpatient ADT	Yes	Yes	Acknowledge

APPENDIX D ï PRIVILEGE MATRIX FOR DIFFERENT USER GROUP FOR DIFFERENT APPLICATION SOFTWARE

Figure 2: Privilege Matrix matching Privileges to Perform Clinical Documentation in CIS-EMR for Nurse and Laboratory Technologist

System	01: **Clinical Information System-EMR**											
Application	Clinical documentation											
User group	**DIRECT CARE PROVIDER (CLINICIAN)**						**CLINICAL SUPPORT PROVIDER**					
	NURSE						LABORATORY TECHNOLOGIST					
Data group	**Privilege for Data Management Functions**						**Privilege for Data Management Functions**					
A Symptoms Signs Diagnosis Lab orders	**Read**		**Write**		**Manipulate**		**Read**		**Write**		**Manipulate**	
	View	Õ	Insert	Õ	Validate	Õ	View	Õ	Insert	**X**	Validate	**X**
	Retrieve	Õ	Submit	Õ	Modify	Õ	Retrieve	Õ	Submit	**X**	Modify	**X**
	Copy	Õ	Record	Õ	Add	Õ	Copy	**X**	Transfer	**X**	Add	**X**
	Duplicate	Õ			Delete	Õ	Duplicate	**X**	Record	**X**	Delete	**X**
	Print	Õ					Print	**X**				

Data group	Privilege for Data Management Functions						Privilege for Data Management Functions					
B Status Result	**Read**		**Write**		**Manipulate**		**Read**		**Write**		**Manipulate**	
	View	Õ	Insert	**X**	Validate	**X**	View	Õ	Insert	Õ	Validate	Õ
	Retrieve	Õ	Submit	**X**	Modify	**X**	Retrieve	Õ	Submit	Õ	Modify	Õ
	Copy		Record	**X**	Add	**X**	Copy	Õ	Transfer	Õ	Add	Õ
	Duplicate				Delete	**X**	Duplicate	Õ	Record	Õ	Delete	**X**
	Print						Print	Õ				

Figure 3: Privilege Matrix matching Privileges to Perform Laboratory Information System Tasks for Laboratory Receptionist and Laboratory Technologist

System	02: **Laboratory Information System**											
Application	Test performance and resulting											
User group	**CLINICAL ADMINISTRATION STAFF**						**CLINICAL SUPPORT PROVIDER**					
	LABORATORY RECEPTIONIST						LABORATORY TECHNOLOGIST					
Data group	**Privilege for Data Management Functions**						**Privilege for Data Management Functions**					
C Log in specimen Reject specimen Review worklist	**Read**		**Write**		**Manipulate**		**Read**		**Write**		**Manipulate**	
	View	Õ	Insert	Õ	Modify	Õ	View	Õ	Insert	Õ	Modify	Õ
	Retrieve	Õ	Submit	Õ	Add	Õ	Retrieve	Õ	Submit	Õ	Add	Õ
	Copy	**X**	Record	Õ	Delete	**X**	Copy	Õ	Transfer	Õ	Delete	**X**
	Duplicate	**X**					Duplicate	Õ	Record	Õ		
	Print	**X**					Print	Õ				

Data group	Privilege for Data Management Functions						Privilege for Data Management Functions					
D Start test End test Task status Result	**Read**		**Write**		**Manipulate**		**Read**		**Write**		**Manipulate**	
	View	**X**	Insert	**X**	Validate	**X**	View	Õ	Insert	Õ	Validate	Õ
	Retrieve	**X**	Submit	**X**	Modify	**X**	Retrieve	Õ	Submit	Õ	Modify	Õ
	Copy	**X**	Record	**X**	Add	**X**	Copy	Õ	Transfer	Õ	Add	Õ
	Duplicate	**X**			Delete	**X**	Duplicate	Õ	Record	Õ	Delete	**X**
	Print	**X**					Print	Õ				

APPENDIX E - USER DESCRIPTION DEFINITION

No.	DESIGNATION	DEFINITION AND ROLES
1.	Nursing Director/ Matron	A nurse who has been designated the responsibility and authority to manage the nursing activities of a hospital or a health district.
2.	Assistant Medical Officer	Healthcare professional who has undergone training and obtained qualification recognized by MOH and registered by the Medical Assistant Board under Medical Assistants (Registration) Act 1977.
3.	Medical Laboratory Technologist	An individual who is trained and registered as a Medical Laboratory Technologist to perform routine and complex laboratory investigations in various disciplines of pathology.
4.	Medical Officer	**Privileges of Fully registered person(Medical Act 1971 No.26)** Every person whose name is for the time being borne on the Register as fully registered under this Act shall be entitled, according to his qualifications, to practice medicine, surgery and midwifery in accordance with the provision of this Act and to recover in due course of law reasonable charges for professional aid, advice and visits and the value of any medicine or any medical or surgical appliances rendered, made of supplied by him to his patients, provided that at the at the time of performing any such act he had an annual practising certificate in force.

No.	DESIGNATION	DEFINITION AND ROLES
		Any contract Medical Professional who have been issued temporary practicing certificate (TPC) to practice medicine for a specified period. **Exemption of certain medical officers in ships(Medical Act 1971, No15)** All ship's surgeons of their duties shall be exempted from registration under this Act and shall be entitled to all the privileges of fully registered medical practitioners under this Act.
5.	Medical Record Officer	A person who has undergone training in management of medical records works in a medical record office of a health facility.
6.	Assistant Medical Record Officer	A person who has undergone training in management of medical records works in a medical record office of a health facility.
7.	Assistant Medical Record	A person who has undergone training in management of medical records works in a medical record office of a health facility assist Assistant Medical Record Officer.
8.	Medical Student (undergraduate)	A person who is undergoing training in medicine and pursuing degree qualification from a recognized institution.
9.	Medical Social Officer	An individual who is trained and registered as a Medical Social Officer to conduct assessment and intervention; manage biopsychosocial problems and provide consultation to individuals, their family members or caregivers.
10.	Non-clinical Administrator	A non-health care professional that is tasked with administrative and financial duties at a health facility.
11.	Staff Nurse	Main functions of the nurse are to give a holistic treatment to the patients in the health facilities such as general wards, operation theatres, outpatient departments and specialist clinics.

No.	DESIGNATION	DEFINITION AND ROLES
12.	Nutritionist	An individual who is trained and registered as a Nutritionist to promote nutritional well being, prevent nutrition-related diseases, conduct nutrition interventions, carry out nutrition or nutrition-related research and development, provide nutritional consultancy and advice, assess and monitor the nutritional status of individuals and communities.
13.	Dietitian	An individual who is trained and registered as a Dietitian to perform nutrition assessment and diagnosis; prescribe medical nutrition therapy; monitor, evaluate and document the nutrition care of individuals and groups requiring diet intervention and rehabilitation; provide diet counseling to individuals and caregivers; manage foodservices including therapeutic diets; and promote wellness in the community and provide consultation to related industries.
14.	Pharmacist	A person, who has undergone training, received a degree qualification in pharmaceutical science and registered under Registration of Pharmacy Act 1951.
15.	Pharmacy Assistant	A person who has undergone training in pharmacy, obtained diploma qualification recognized by MOH and registered by the Pharmacy Board. A person who practice under supervision of a pharmacist
16.	Diagnostic Radiographer	An individual who is trained and registered as a Diagnostic Radiographer to acquire and interpret medical images using ionising radiation and other imaging modalities for medical diagnostic and interventional purposes.
17.	Researcher ü Clinical ü Public Health ü Health Economics	A professional in a field related to health who is undertaking an authorized study / research project in a health & pharmaceutical sector.
18.	Scientific Officer	A person, who has undergone training, received a degree qualification in a scientific field and working in a health facility. They included Biochemist, Microbiologist, Physicist, Genetics, Entomologist, Embryologist, Forensic, Food Nutrition & Biomedical.

No.	DESIGNATION	DEFINITION AND ROLES
		Principal role: Conducts medical laboratory tests as well as processing samples and interpreting medical results to assist in the diagnosis, treatment and prevention of disease.
19.	Clinical Scientist (Biochemist)	An individual who is trained and registered as Clinical Scientist (Biochemist) to conduct analysis and technical interpretation of data in the area of clinical biochemistry and its related fields, setting standard and monitoring of performance of diagnostic investigations, evaluation and selection of methods, instruments and technologies.
20.	Clinical Scientist (Biomedical Science)	An individual who is trained and registered as a Clinical Scientist (Biomedical Science) to conduct diagnostic investigation in areas of clinical pathology including hematology, histopathology, cytopathology, microbiology, chemical pathology and transfusion services, selection and develop advanced technologies and methodologies and monitoring of laboratory setting for quality control.
21.	Clinical Scientist (Embryologist)	An individual who is trained and registered as a Clinical Scientist (Embryologist) to perform all laboratory aspects of assisted human reproductive technologies.
22.	Clinical Scientist (Medical Geneticist)	An individual who is trained and registered as a Clinical Scientist (Medical Geneticist) to perform cytogenetic, molecular genetics and biochemical genetics applications for diagnosing diseases, to provide advice in the related application protocol, to use his scientific skills in experimental designs and problem solving and in service development through research and investigations.
23.	Clinical Scientist (Microbiologist)	An individual who is trained and registered as Clinical Scientist (Microbiologist) to detect and identify bacteria, virus, fungi and parasites, develop and implement methodologies, maintain quality performance, provide analytical result of microbiological and immunological investigations for the purpose of disease diagnosis, treatment and surveillance.
24.	Entomologist	An individual who is trained and registered as an Entomologist to conduct technical field inspections and laboratory studies directed at the identification, classification and control of insects that may have an adverse effect on the environment and health.

No.	DESIGNATION	DEFINITION AND ROLES
25.	Forensic Science Officer	An individual who is trained and registered as a Forensic Science Officer to conduct medico legal forensic investigations in laboratories and crime scene.
26.	Healthcare Foodservice Officer	An individual who is trained and registered as a Healthcare Foodservice Officer to manage foodservice operation in healthcare facilities, management of food production for normal and therapeutic diets, procurement of food and catering facilities, menu planning, budgeting, formulate policies and procedures for safety of food.
27.	Medical Physicist	An individual who is registered and trained as a Medical Physicist to conduct quality control of imaging and / or therapeutic radiation facilities and perform duties in nuclear medicine, radiotherapy, radiology and cyclotron facilities.
28.	Nurse Unit Manager/Sister	A nurse who has been designated to be in-charge in a specified area of nursing in a health facility or district.
29.	Specialist	A registered medical / dental practitioner who has undergone the required training and acquired the necessary qualification to practice in a specialized area of medicine/ dentistry. Any foreign specialist who have been issued temporary practicing certificate (TPC) to practice medicine for a specified period.
30.	Physiotherapist	An individual who is trained and registered as a Physiotherapist to promote, prevent, analyze, make physiotherapy diagnosis, carry out physiotherapy treatment, intervene, habilitate and rehabilitate of any form of physical conditions and disabilities to restore optimum movement and functional abilities.

No.	DESIGNATION	DEFINITION AND ROLES
31.	Occupational Therapist	An individual who is trained and registered as an Occupational Therapist to prevent, promote, make occupational therapy diagnosis and provide occupational therapeutic interventions for individuals who are physically and / or psychosocially impaired to enhance performance through engagement and participation in activities of daily living, work and leisure.
32.	Radiation Therapist	An individual who is trained and registered as a Radiation Therapist to perform radiotherapy imaging, develop, evaluate and verify treatment plans; to deliver the planned and prescribed treatment using accurate and safe radiation therapy; and to monitor and assess radiation side effects, with the aim of cure and palliation of diseases treated with radiotherapy.
33.	Speech-Language Therapist (speech pathologist)	An individual who is trained and registered as a Speech-Language Therapist managing individuals with speech, language, voice, communication, feeding and swallowing disorders through appropriate speech-language pathology modalities of screening, assessment, diagnosis, intervention, therapy, counseling, consultation, prevention and education.
34.	Dental Officer	A registered dental practitioner who is licensed to practise dentistry under the provision of the Dental Act 1971.
35.	Dental student (undergraduate)	A person who is undergoing training in dentistry and pursuing degree qualification from a recognized institution.
36.	Dental Surgery Assistant	Healthcare personnel who has undergone training and obtained qualification recognized by MOH. Role: Helps the dental officer or dental nurse in the management of patients, responsible for infection control in the dental surgery, register patients, Collect payment from patients and issue receipts, and manage patient records.
37.	Dental Nurse	Healthcare professional who has undergone training and obtained qualification recognized by MOH Role: A dental nurse practice dentistry under the supervision of a registered dental surgeon in any hospital, clinic, or dental school approved for the purpose by the Minister.

No.	DESIGNATION	DEFINITION AND ROLES
38.	Dental Therapist	Means an individual who is trained and registered as a Dental Therapist, who works under the direct supervision of Dental Surgeon in the private sector or under direct/indirect supervision of a Dental Surgeon in the public sector to provide promotive, preventive and basic clinical dental care.
39.	Dental Technologists	An individual who is trained and registered in the Register of Dental Technologists, who works under prescription of a Dental Practitioners, to fabricate dental appliances, dental restorative devices and maxilla-facial prostheses for the rehabilitation of oral function. Healthcare personnel who has undergone training in dental technology and obtained qualification recognized by MOH. Role: Manufacture dental prosthetics including orthodontic appliances, crowns and bridges, complete/partial dentures and maxillofacial prosthesis according to specifications by dental surgeons/specialist. Also responsible for the repair and maintenance of dental equipment.
40.	Healthcare Assistant	Healthcare personnel who has undergone specific in-house training and fit for purpose.
41.	Environmental Health Officer	An individual who is trained and registered as an Environmental Health Officer to prevent environmental health hazard and the promotion and protection of the public health and the environment in the following areas of disease control; food hygiene and safety; housing; institutional environmental health; vector control; drinking water quality; water sanitation; emergency preparedness; enforcing public health legislation in tandem with the roles and functions as stipulated by the Expert Committee to the World Health Organization Report No. 79, or amendments made thereto.
42.	Counseling Officer	Healthcare personnel who has undergone diploma or degree qualification and obtained qualification recognized by MOH/JPA.

No.	DESIGNATION	DEFINITION AND ROLES
43.	Clinical Psychologist	means an individual who is trained and registered as a Clinical Psychologist to deal with research and clinical application of psychological principles for the recognition, assessment, diagnosis, treatment, rehabilitation and prevention of cognitive, emotional, behavioral and learning disorders to enhance subjective well-being, mental health and life functioning.
44.	Hospital Director	Healthcare personnel who is incharge of hospital, organisation or activity and give instruction and direction.
45.	Head Of Department	Healthcare personnel who is head of Department/Unit and has administration responsibility for unclassified faculty/staff member
46.	Family Medicine Specialist	A Registered Family Physician who has undergone the required training, special emphasis is place on the primary care of families.
47.	Houseman Officer	Means a medical practitioner undergoing internship training under the Malaysia Act 1971. „ I n t e r n s h i p " i s t h e p e r i o d o f r e s i d e n t m e d i c a l p r Act 1971.
48.	Community Nurse	The main task of community nurse concentrated in the area of obstetrics and family health which include aspects of nursing care in nursing practice, nursing management, nursing training, documentation and other tasks.
49.	Optometrist	Healthcare professional who has undergone training and obtained qualification recognized by MOH and registered by the (Majlis Optik Malaysia) MOM.
50.	Audiologist	An individual who is trained and registered as an Audiologist to provide a comprehensive array of professional services related to the prevention of hearing loss, audiologic identification, assessment, diagnosis and intervention of persons with impairment of auditory and vestibular functions.

No.	DESIGNATION	DEFINITION AND ROLES
51.	Health Education Officer	An individual who is trained and registered as a Health Education Officer to conduct individual and community needs assessment, behavioral diagnosis for health education / health promotion, plan and implement appropriate health education / health promotion interventions strategies in healthcare facilities and community, conduct appropriate evaluations and research with the aim to empower people by developing individual skills and creating supportive environment
52.	Lecturers/Tutors/ Preceptors	Someone who teaches at a college or university
53.	System Administrator	Is a person employed to maintain and operate a computer system and/or network. System administrators may be members of an information technology (IT) or Electronics and Communication Engineering department.

* Sources: Final draft Allied Health Act, Legal advisor, MOH; Medical Development Division, MOH; Dental Health Division, MOH; Pharmacist Division, MOH; Medical Assistants (Registration) Act 1977. Medical Act 1971. Training Management Division,MOH.

APPENDIX F ï GLOSSARY OF TERMS I

No.	DESIGNATION	DEFINITION
1.	Allied Health Profession Students	A person, who has undergone training in allied Health and pursuing, degree qualification from a recognized institution
2.	Courts	1. **"Court"** means any court in Malaysia of competent jurisdiction, and includes any Judge thereof whether sitting in Court or in chambers; CIVIL LAW ACT 1956 (REVISED 1972) [ACT 67] 2. **"Court"** means a court of competent jurisdiction **INTERPRETATION ACTS 1948 AND 1967 (CONSOLIDATED AND REVISED 1989) [ACT 388]** 3. **Court** A governmental body consisting of one or more judges who sit to adjudicate disputes and administer justice. **B l a c k l a wô s th Edition i o n a r y 8**
3.	Custodian of information	A person who has responsibility for taking care of or protecting the information
4.	Employer	1. "Employer" means any person who engages a worker and includes the agent, manager or factor of such employer; [ACT 246] PRIVATE EMPLOYMENT AGENCIES ACT 1981 2. "Employer" means the person with whom an employee has entered into a contract of service or

No.	DESIGNATION	DEFINITION
		apprenticeship and includes- (a) a manager, agent or person responsible for the payment of salary or wages to an "employee"; (b) any body of persons whether or not statutory or incorporated; and (c) any Government, department of Government, statutory bodies, local authorities or other bodies specified in the Second Schedule and, where an employee is employed with any such Government, department, authority or body or with any officer on behalf of any such Government, department, authority or body, the officer under whom such employee is working shall be deemed to be an employer: Provided that no such officer shall be personally liable under this Act for anything done or omitted to be done in good faith by him as an officer of such employer; **[ACT 452] EMPLOYEES PROVIDENT FUND ACT 1991** 3. "Employer" means any person or body of persons, whether corporate or unincorporate, who employs a workman under a contract of employment, and includes the Government and any statutory authority, unless otherwise expressly stated in this Act; **[ACT 177] INDUSTRIAL RELATIONS ACT 1967** 4. "Employer" means any person who engages a worker and includes the agent, manager or factor of such employer; **[ACT 246] PRIVATE EMPLOYMENT AGENCIES ACT 1981** 5. "Employer" includes the Government of Malaysia and the Governments of each of the States; in respect of civilian employees engaged in Malaysia or in Singapore of any visiting force lawfully present in Malaysia or of any person in the civil employment of the Government of any Commonwealth country, whose contract of service was made in Malaysia or in Singapore, the Government of that Commonwealth country; any local authority; any person or body of persons whether statutory or incorporated or not; the

No.	DESIGNATION	DEFINITION
		legal personal representative of a deceased employer; and in relation to a person employed for the purpose of any game or recreation and engaged or paid through a club, the manager or members of the managing committee of the said club: Provided that where the services of a workman are temporarily lent or let on hire to another person by the person with whom the workman has entered into a contract of service or apprenticeship, the latter shall, for the purposes of this Act, be deemed to continue to be the employer of the workman whilst he is working for that other person; **[ACT 273] WORKMENS COMPENSATION ACT 1952 (REVISED 1982)** 6. "Employer" means any person who has entered into a contract of service to employ any other person as an employee and includes the agent, manager or factor of such first mentioned person, and the word "employ", with its grammatical variations and cognate expressions, shall be construed accordingly; **[ACT 265] EMPLOYMENT ACT 1955 (REVISED 1981)**
5.	Health Care Providers(HCP)	Generic term to reflect all medical practitioners, nurses, medical assistants and allied health professionals.
6.	Insurance Companies	A corporation or association that issues insurance policies. **Black's Law Dictionary 8th Edition**
7.	Legal Guardian	A person who is legally empowered to act on behalf of an individual patient: ¶ A parent whose child is below the age of 18 years ¶ A parent whose child is mentally incapacitated ¶ A legally appointed person (by court of law).

No.	DESIGNATION	DEFINITION
		1. "Guardian" in relation to a child, includes any person who, in the opinion of the Court For Children having cognizance of any case in relation to the child or in which the child is concerned, has for the time being the charge of or control over the child. **CHILD ACT 200 [Act 611]** **2. ñGuardianò** A person having the right and duty of protecting the person, property or rights of one who is without full legal capacity or otherwise incapable of managing his own affairs. (1) Guardianship in chivalry was the right of the lord to hold the land, of an infant tenant until majority. (2) Guardianship in socage was the right of the next of blood to whom the inheritance could not descend, to the wordship of the land while the heir was under the age of 14. (3) Guardianship by nature was that exercised by a father over the person of his son and heir apparent. (4) A guardian by election is one chosen by a minor himself. (5) A guardian by statute is one appointed by will pursuant to the statute. (6) A guardian ad litem is a person appointed to defend an action or other proceeding on behalf of a minor or person under a disability. **CLJ LAW DICTIONARY**

No.	DESIGNATION	DEFINITION
8.	Patient	1. **"Patient"** means a person registered as an outpatient or admitted as inpatient or admitted under the order of the Medical Director, medical officer, registered medical practitioner or upon the order of the Court under the Act. MENTAL HEALTH REGULATIONS 2010 2. **"Patient"** means a person accepted on either an inpatient or outpatient basis. **PRIVATE HEALTHCARE FACILITIES AND SERVICES (PRIVATE HOSPITALS AND OTHER PRIVATE HEALTHCARE FACILITIES) REGULATIONS 2006** **"Patient"** means an individual in the terminal stage of illness who has an anticipated life expectancy of days, weeks or less than six months and who, alone or in conjunction with a family member or members, has voluntarily requested admission and has been accepted into a hospice or palliative care services programme; **PRIVATE HEALTHCARE FACILITIES AND SERVICES (PRIVATE HOSPITALS AND OTHER PRIVATE HEALTHCARE FACILITIES) REGULATIONS 2006**

APPENDIX G - GLOSSARY OF TERMS II

Term	Definition	Source
Separation of duties	By virtue user being authorized as a member of one role, the user is not authorized as a member of second role.	Cugini, D. Richard Khun, Role – Based Access Control (RBAC): Features and Motivations, National Institute of Standards and Technology, U.S. Department of Commerce Gaithersburg MD 20899
Mutual exclusivity	The same user can be assigned to at most one role in a mutually exclusive set. This support separation of duties.	Ravi S. Sandhu, et al., Role-Based Access Control Models, IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.
Cardinality	Some roles can only be occupied by a certain number of employees at any given period of time.	David F. Ferrialo, Janet A. Cugini, D. Richard Khun, Role – Based Access Control (RBAC): Features and Motivations, National Institute of Standards and Technology, U.S. Department of Commerce Gaithersburg MD 20899

APPENDIX H: TASK FORCE AND LIST OF CONTRIBUTORS FOR THE DEVELOPMENT OF THE USER ACCESS CONTROL POLICY (UACP) FOR HOSPITAL/ CLINICAL INFORMATION SYSTEMS (HIS/CIS)

ADVISOR:

Y. Bhg. Dato' Sri Dr. Hasan Bin Abdul Rahman

CHAIRMAN OF TASK FORCE:

Dr. Amiruddin Bin Hisan

FASILITATORS:

En. Chan Peng Wah
Dr. Leela V Sabapathy
Mr. Abdollah Bin Salleh
Dr. Ahmad Fairuz Bin Mohamed
En. Samsuil Fuad Bin Munap
Dr. Dang Siew Bing
Pn. Wan Roshidah bt Wan Ismail

SECRETARIAT:

En. Asraful Kamal Bin Ariffin
Matron Khalijah Binti Dalip
Matron Rozah Binti Ahmad
En. Hussin b Ahmad
En. Zamri b Ahmad
En. Jazmi b Md Sani
En. Kamaruzaman b Che Lah
Tn. Hj. Mohd Zaki Bin Sulaiman
En. Mohd Said Bin Morad
Sister Jamilah bt Abdollah
En. Mohd Norhisham Ismail
En. Mohd Khairuddin Bin Mokhtar
En. Mohd Rizuwan Bin Abdullah

STAGE 1 : PREPARATION OF THE DRAFT ON USER ACCESS CONTROL POLICY FOR HIS/CIS

USER ACCESS CONTROL POLICY WORKSHOP WITH SELECTED REPRESENTATIVES OF CLINICIANS FROM HIS/CIS FACILITIES & RELATED DIVISIONS OF MOH

Participants :

No.	Name	Job Title	Name of Organisation
1.	Mr. Abdollah Bin Salleh	Pakar Bedah Am & Clinical IT Coordinator	Hospital Selayang
2.	Dr. Fekriah Binti Mohd Yatim	Timbalan Pengarah	Bahagian Kesihatan Pergigian KKM
3.	Dr. Norizah Binti Haji AB Ghani	Timbalan Pengarah (Klinikal)	Hospital Tuanku Jaafar Seremban
4.	Dr. Wan Ahmad Hazim Wan Ahmad	Pakar Perunding Kanan O&G	Hospital Putrajaya
5.	Dr. Baizurah Binti Mohd Hussain	Pakar Perunding Pathology	Hospital Ampang
6.	Dr. Malek Faris Riza Feisal Bin Jeffrizal	Pakar Perubatan	Hospital Putrajaya
7.	Dr. Yusniza Binti Mohd Yusof	Pakar Perubatan Rehabilitasi	Hospital Tuanku Jaafar Seremban
8.	Dr. Ahmad Taufik Bin Mohd Jamil	Ketua Pusat Teknologi Maklumat	Pusat Perubatan UKM
9.	Dr. Mazni Bin Mat Junus	Pakar Psikiatri	Hospital Serdang
10.	Dr. Razak Othman	Pakar Psikiatri	Hospital Sungai Buloh

11.	Dr. Azlina Bin A.Rahman	Pakar Trauma & Kecemasan	Hospital Ampang
12.	Dr. Zainal Fitri Bin Zakaria	Pakar Kesihatan Keluarga	Klinik Kesihatan Putrajaya
13.	Dr. Mohd Fauzi bin Abu Bakar	Pegawai Perubatan	Klinik Kesihatan Putrajaya
14.	Puan. Sharifah Salwa Syed Abu Bakar	Pengurus Besar-Jabatan Pengurusan IT	Institut Jantung Negara
15.	Dr. Shahabudin Bin Ibrahim	Ketua Pen. Pengarah Kanan	Bahagian Amalan Perubatan
16.	Cik Kogilavani a/p Munusamy	Pegawai Teknologi Maklumat	Klinik Kesihatan Putrajaya
17.	Tn. Hj. Sarudin Bin Zainul	Pen. Pegawai Perubatan	Hospital Selayang
18.	Puan Zarina Ripin	Pen. Pegawai Teknologi Maklumat	Hospital Selayang
19.	Pn. Umi Kalsom Binti Adam	Ketua Pen. Setiausaha Kanan	Bahagian Pengurusan Maklumat
20.	Matron Sin Lian Thye	Penyelia Jururawat	Bahagian Perkembangan Perubatan
21.	Matron Khuzaifah Bin Mohd Noh	Penyelia Jururawat	Bahagian Perkembangan Perubatan
22.	Syahir Bin Shaffie	Kerani Kaunter Pendaftaran Pesakit	Hospital Tuanku Jaafar Seremban

STAGE 2 : TO OBTAIN A WIDER CONSENSUS ON THE DRAFT POLICY

USER ACCESS CONTROL POLICY FORUM

Participants :

No.	Name	Job Title	Name of Organisation
1.	Mr. Abdollah Bin Salleh	Pakar Bedah Am & Clinical IT Coordinator	Hospital Selayang
2.	Dr. Heselynn Binti Hussein	Ketua Jabatan Perubatan & Pakar Perunding Perubatan	Hospital Putrajaya
3.	Dr. Wan Ahmad Hazim Wan Ahmad	Pakar Perunding Kanan O&G	Hospital Putrajaya
4.	Pn. Kamarunnesa Binti Mokhtar Ahmad	Ketua Jabatan Farmasi & Pegawai Farmasi	Hospital Putrajaya
5.	Cik Rubaizah Binti Yatim	Ketua Jabatan Teknologi Maklumat	Hospital Putrajaya
6.	Dr. Baizurah Binti Mohd Hussain	Pakar Perunding Pathology	Hospital Ampang
7.	Dr. Faizatuddarain Binti Mahmood	Pakar Radiologi	Hospital Ampang
8.	Dr. Nurmaimun Musni	Pegawai Perubatan	Hospital Ampang
9.	Dr. Hajah Zainab Binti Ramli	Timbalan Pengarah (Surgikal)	Hospital Tengku Ampuan Rahimah Klang
10.	Dr. Ahmad Tajuddin Bin Mohamad Nor	Pakar Perunding Jabatan Kecemasan	Hospital Tengku Ampuan Rahimah Klang

11.	Dr. Hisham Kunhimon	Pakar Bedah Ortopedik	Hospital Selayang
12.	En. Sarudin Bin Zainul	Pen. Pegawai Perubatan	Hospital Selayang
13.	Mr. Muralee Madhavan	Pakar Ortopedik	Hospital Serdang
14.	En.Nizalene Deliza bin Husaini	Pegawai Teknologi Maklumat	Hospital Serdang
15.	Dr. Husni Binti Husain	Pakar Perubatan Kesihatan Keluarga	Klinik Kesihatan Putrajaya
16.	Cik Nazhiyah Binti Haron	Pegawai Teknologi Maklumat	Pejabat Kesihatan Daerah Putrajaya
17.	Dr. Ahmad Taufik Bin Mohd Jamil	Ketua Pusat Teknologi Maklumat	Pusat Perubatan UKM
18.	En. Mohamad Bin Zainudin	Pegawai Teknologi Maklumat	Pusat Perubatan UKM
19.	Pn. Kamariah Binti Md Nasir	Pegawai Teknologi Maklumat	Pusat Perubatan UKM
20.	En. Saravanan a/l Rajagopal	Pegawai Teknologi Maklumat	Hospital Sultan Haji Ahmad Shah, Kuantan
21.	Pn. Hamidah Binti Karim	Pen. Pegawai Rekod Perubatan	Hospital Sungai Buloh
22.	Pn. Siti Zamnah Binti Mohammed Zaki	Pen. Pegawai Tadbir	Hospital Sungai Buloh
23.	En. Rajali Halidi	Pen. Pegawai Takbir Rekod	Hospital Port Dickson
24.	En. Jaafar Jamaan	Timbalan Setiausaha Bahagian	Bahagian Pengurusan Maklumat, KKM

25.	Datin Jawahiril Kamariah Binti Mohamad	Timbalan Setiausaha Bahagian	Bahagian Pengurusan Maklumat, KKM
26.	En. Jaafar Bin Ahmad	Ketua Penolong Setiausaha Kanan	Bahagian Pengurusan Maklumat, KKM
27.	Pn. Wan Mahani binti Wan Ismail	Ketua Penolong Setiausaha Kanan	Bahagian Pengurusan Maklumat, KKM
28.	Dr. Azizah Binti Arshad	Ketua Penolong Pengarah Kanan	Bahagian Perkembangan Perubatan, KKM
29.	Matron Khuzaifah Bin Mohd Noh	Penyelia Jururawat	Bahagian Perkembangan Perubatan, KKM
30.	Matron Sin Lian Tyhe	Penyelia Jururawat	Bahagian Perkembangan Perubatan, KKM
31.	Dr. Fekriah Binti Mohd Yatim	Timbalan Pengarah	Bahagian Kesihatan Pergigian KKM
32.	Sister Cheng Chue Chu	Ketua Jururawat Pergigian	Bahagian Kesihatan Pergigian KKM
33.	Dr. Shahabudin Bin Ibrahim	Ketua Pen. Pengarah Kanan	Bahagian Amalan Perubatan, KKM
34.	Dr. Sharfudin Bin Noordin	Timbalan Pengarah	Bahagian Amalan Perubatan, KKM
35.	Cik Nasitah Binti Sani	Pen. Pegawai Teknologi Maklumat	Bahagian Amalan Perubatan, KKM

36.	En. Jamalul Rijal Bin Abd. Aziz	Pegawai Teknologi Maklumat	Pusat Informatik Kesihatan, KKM
37.	Dr. Ilias Bin Adam Yee	Penolong Pengarah Kanan	Pusat Informatik Kesihatan, KKM
38.	Dr. Azrulreezal Azannee Bin Abdul Wahab	Penolong Pengarah	Pusat Informatik Kesihatan, KKM
39.	Dr. Fathullah Iqbal Bin Ab. Rahim	Penolong Pengarah	Pusat Informatik Kesihatan, KKM
40.	Puan Noorsiah Binti Hassan Basri	Pegawai Tadbir Rekod Perubatan	Bahagian Perancangan Dan Pembanggunan
41.	Cik Lidyawati Binti Abdul Hamid	Pegawai Teknologi Maklumat	Bahagian Perancangan Dan Pembanggunan
42.	Puan Narimah Binti Moris	Peguam Kanan Persekutuan	Penasihat Undang-Undang
43.	Dr. Sarie I d h a d h y u `	Penolong Setiausaha	Majlis Perubatan Malaysia

STAGE 3: TO REVIEW & OBTAIN THE APPROVAL FROM THE NATIONAL HEAD OF SERVICES, MOH

USER ACCESS CONTROL POLICY MEETING WITH HEAD OF NATIONAL SERVICES, MINISTRY OF HEALTH

Members at the meeting :

No.	Name	Job Title	Name of Organisation
1.	Mr. Abdollah Bin Salleh	Pakar Bedah Am & Clinical IT Coordinator	Hospital Selayang
2.	Dato' Dr. Omar Ismail	Pakar Perunding Kardiologi	Hospital Pulau Pinang
3.	Dato' Dr. Jeyaindran Tan Sri Sinnadurai	Pakar Prunding Kanan Perubatan	Hospital Kuala Lumpur
4.	Dato' Dr. N. Premchandran a/l P.S. Menon	Pakar Perunding Kanan Orthopedic	Hospital Tuanku Ampuan Afzan
5.	Dr. Hussin Imam Hj. Muhammad Ismail	Pakar Perunding Kanan Pediatrik	Hospital Kuala Lumpur
6.	Mr. Johari Siregar Adenan	Pakar Perunding Neurosurgery	Hospital Sultanah Aminah Johor
7.	Datin Dr. Zaharah Musa	Pakar Perunding Radiologi	Hospital Selayang
8.	Dr. Basir Towel	Pakar Perunding Kanan Orthopedic	Hospital Serdang
9.	Pn. Narimah Moris	Penasihat Undang-undang Kanan	Penasihat Undang-undang KKM
10	Dr. Heselynn Binti Hussein	Ketua Jabatan Perubatan & Pakar Perunding	Perubatan Hospital Putrajaya

11.	Dr. Wan Ahmad Hazim Wan Ahmad	Pakar Perunding Kanan O&G	Hospital Putrajaya
12.	Dr. Zainal Fitri Bin Zakaria	Pakar Kesihatan Keluarga	Klinik Kesihatan Putrajaya
13.	Dr. Baizurah Binti Mohd Hussain	Pakar Perunding Pathology	Hospital Ampang
14.	Cik Rubaizah Binti Yatim	Ketua Jabatan Teknologi Maklumat	Hospital Putrajaya
15	Cik Nazhiyah Binti Haron	Pegawai Teknologi Maklumat	Pejabat Kesihatan Daerah Putrajaya
16	Dr Leela V Sabapathy	Timbalan Pengarah,	Bahagian Telekesihatan
17.	En. Samsuil Fuad Bin Munap	Timbalan Pengarah	Bahagian Telekesihatan

ACKNOWLEDGEMENT

Dr Ong Chee Leng, Deputy Director Telehealth Division has been instrumental in the initial work for the formulation of this User Access Control policy.

REFERENCES

1. http://en.wikipedia.org/wiki/Access_control/21072011
2. http://en.wikipedia.org/wiki/Role-based_access_control/21072011
3. HL7 Role-Based Access Control (RBAC) Role engineering Process/Version 1.3/HL7 Security Technical Committee/ September 2007