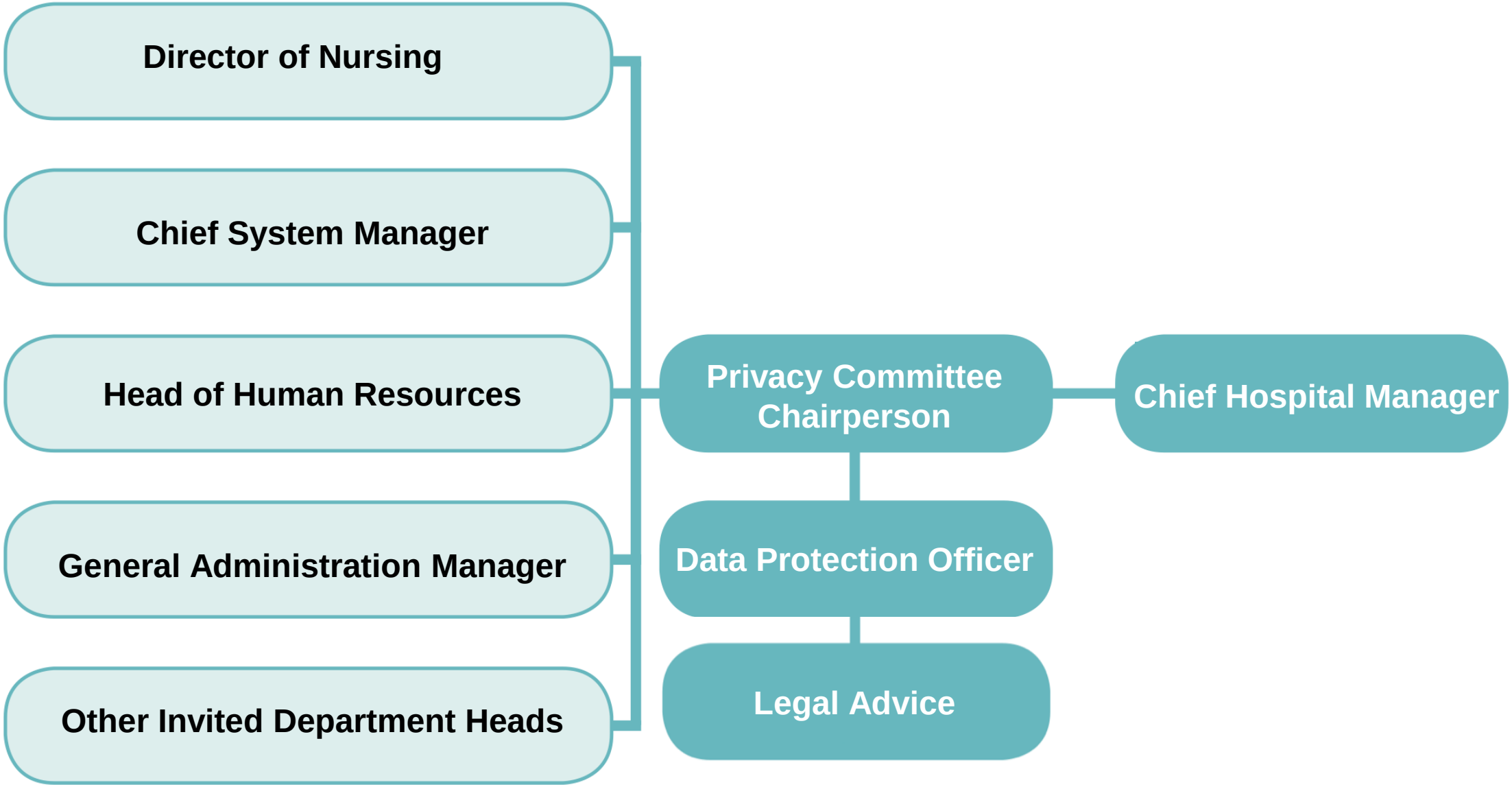
仁安醫院
UNION HOSPITAL

Privacy Committee

仁安醫院 UNION HOSPITAL




仁安醫院
UNION HOSPITAL
Email
仁安醫院
UNION HOSPITAL
UNION HOSPITAL
Agenda of the 23rd Privacy Committee Meeting (BIANNUAL)
Date: 3rd January 2024 (Wednesday)
Time: 3:00 p.m.
Venue: New Seminar Room 1
The following matters will be discussed:
1. Matters Arising from the Last Minutes

仁安醫院
UNION HOSPITAL

UNION HOSPITAL

Agenda of the 23rd Privacy Committee Meeting (BIANNUAL)

Date: 3rd January 2024 (Wednesday)

Time: 3:00 p.m.

Venue: New Seminar Room 1

The following matters will be discussed:

1. Matters Arising from the Last Minutes
2. Review of Cases related to Privacy
3. Privacy Training
4. Personal Information Collection Statement Review
5. Cybersecurity
6. Review of the Privacy Management System


仁安醫院
UNION HOSPITAL
Intranet
第23次私隱委員會 (Privacy Committee) 會議記錄
仁安醫院
UNION HOSPITAL
日 期 ： 2024 年 1 月 3 日 (星期三)
時 間 ： 下午3時
地 點 ： New Seminar Room 1
出席者 ：何健基醫生 QAT (主席)
[redacted]總監 NUA
[redacted]先生 ITS
[redacted]先生 HRD
[redacted]先生 ADM
[redacted]小姐 PHA
[redacted]小姐 CIM
缺席者 ：[redacted]小姐[redacted] ITS
會議記錄:
跟進
1. 主席及與會代表通過第22次會議記錄。


仁安醫院
UNION HOSPITAL
Intranet
第23次私隱委員會 (Privacy Committee) 會議記錄
仁安醫院
UNION HOSPITAL
3.5 個人資料私隱管理系統評估
主席指出，倘若個人資料交由外判商處理時被洩漏，仍需由本院承擔責任，因此提醒與會者需要在合約上小心列明條款，並只與信譽良好的商家及廠商合作。


仁安醫院
UNION HOSPITAL
CERTIFIED
ISO
9001:2015
COMPANY

Regular Review of Privacy Policy

Regular Review of the Personal Information Collection Statement (PICS) on the Registration Charts & Hospital Posters

仁安醫院
UNION HOSPITAL

Privacy Training Videos for Pre-Employment Training with MCQ & Logging

仁安醫院
UNION HOSPITAL

Employee Confidentiality Agreement

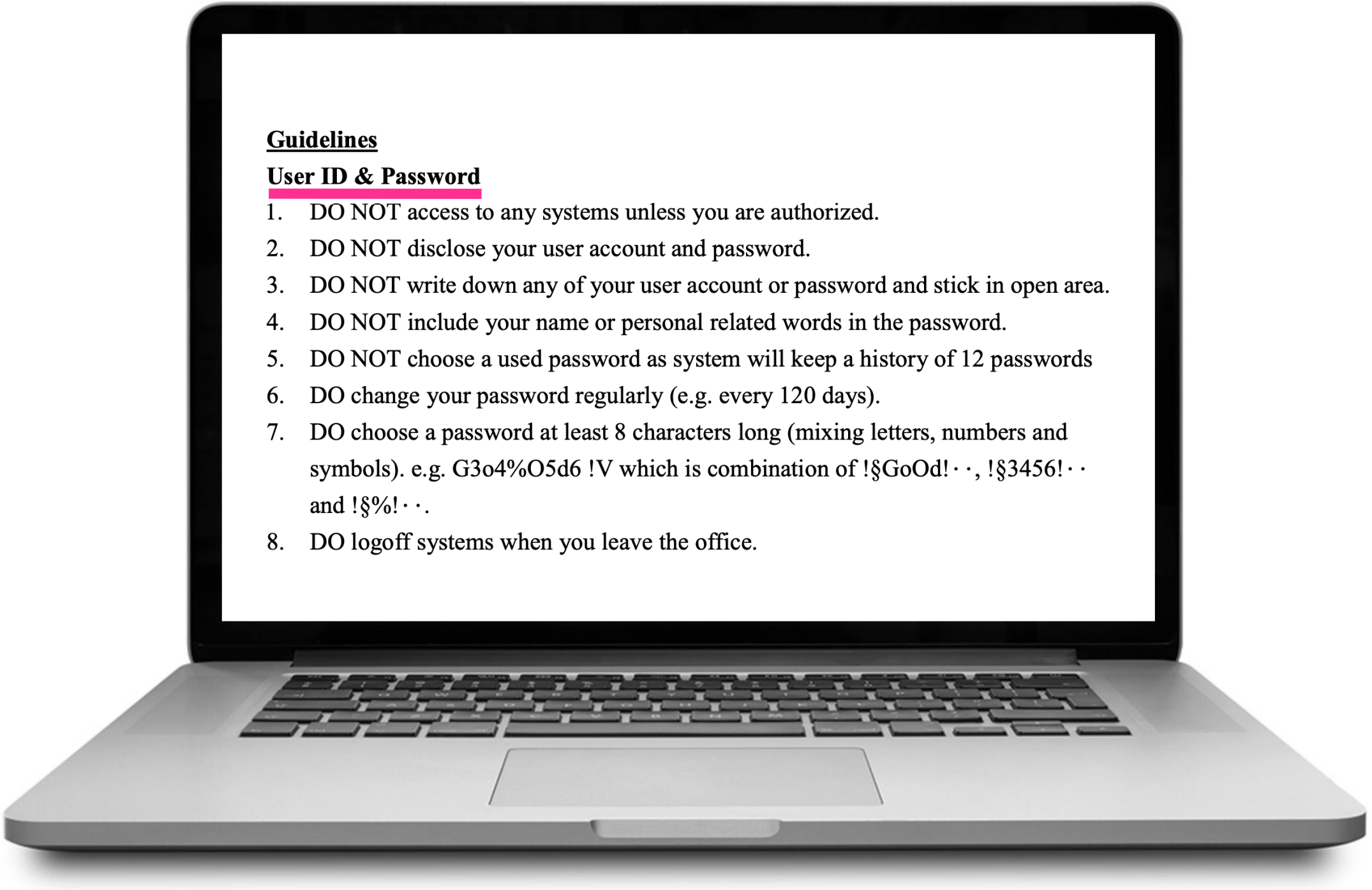
This is an agreement between the Union Hospital and _____ [Name of Employee]

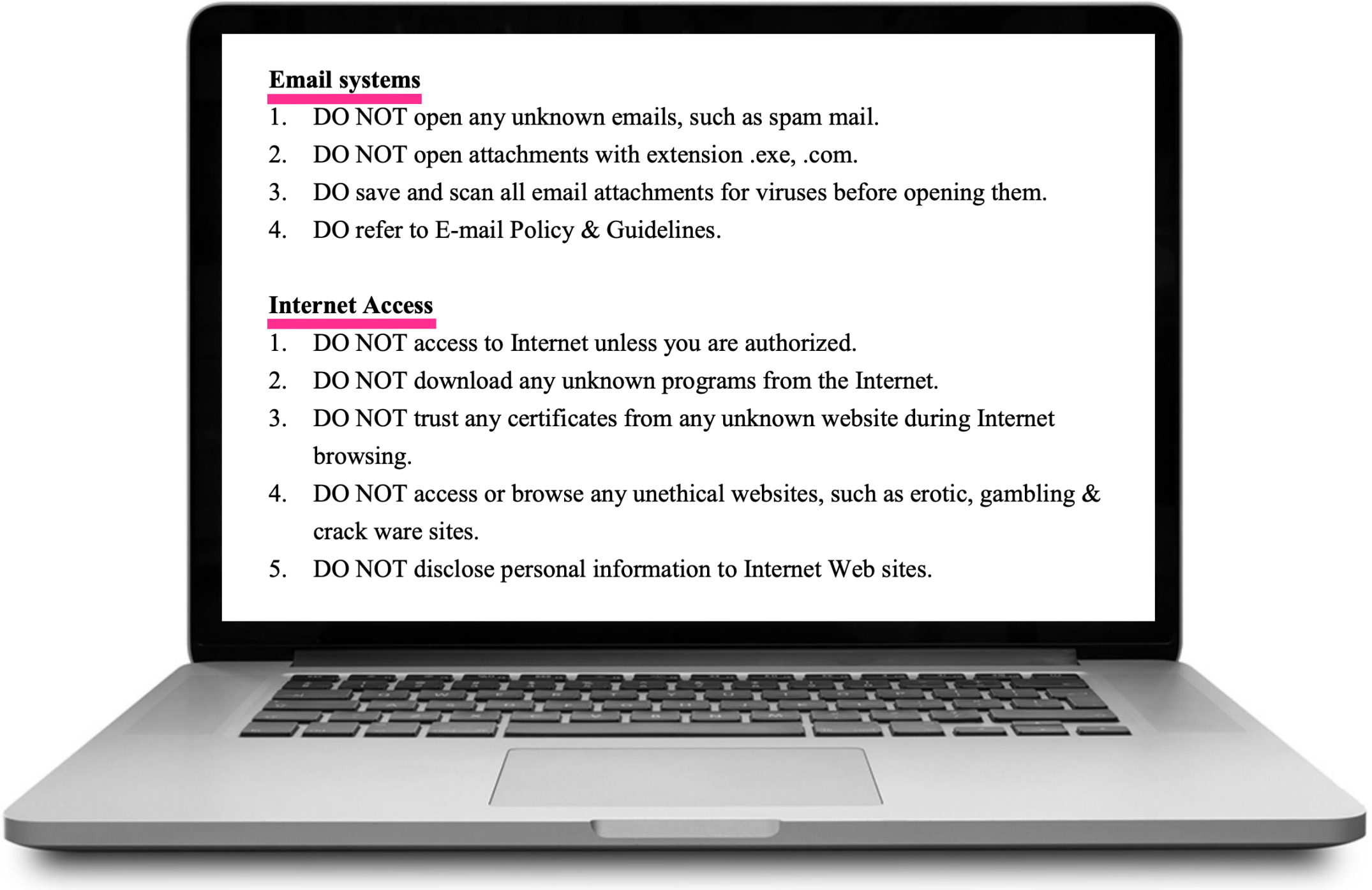
Online Privacy & Staff Behaviour Training for New Staff with Logging

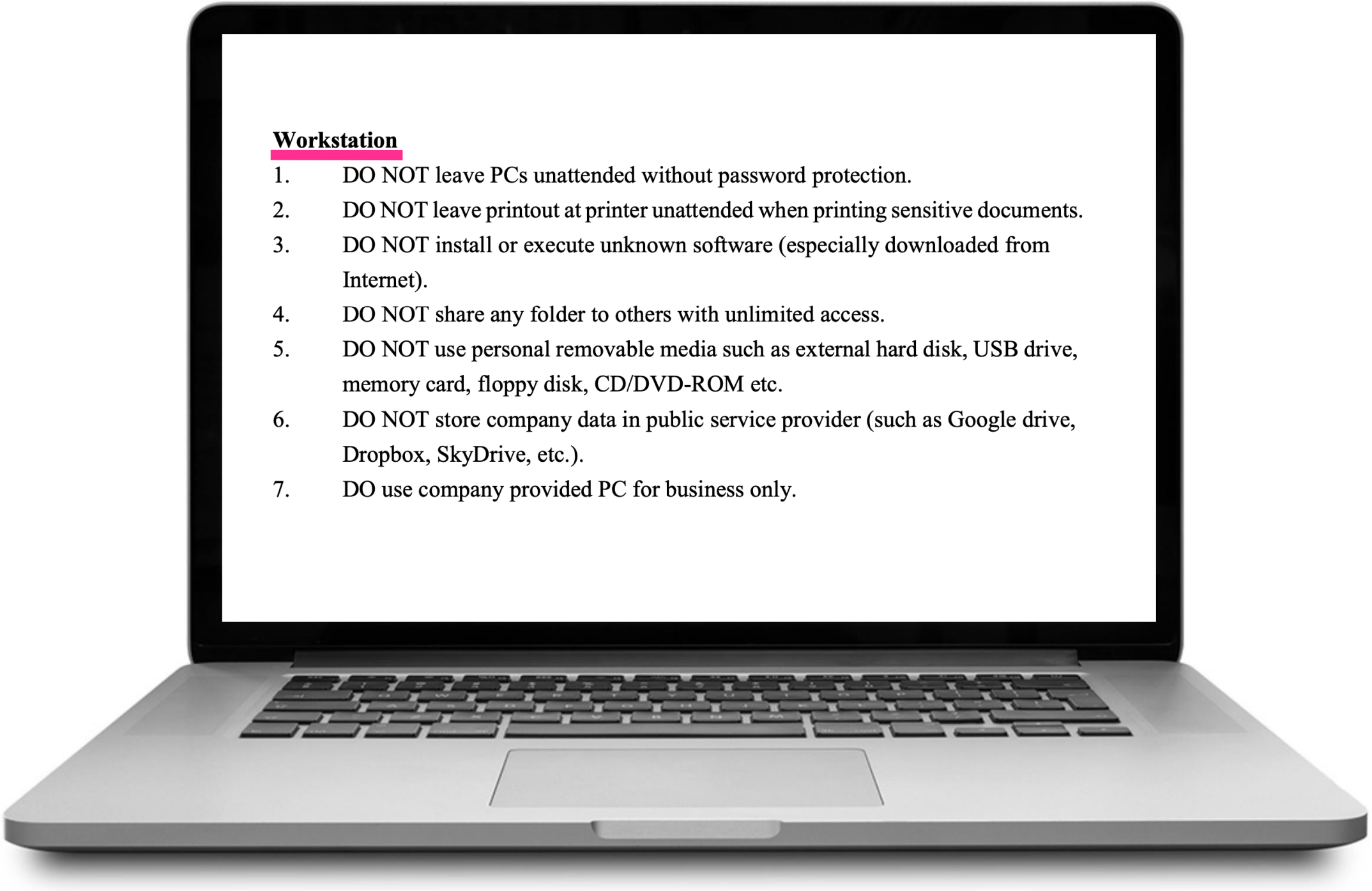
仁安醫院
UNION HOSPITAL

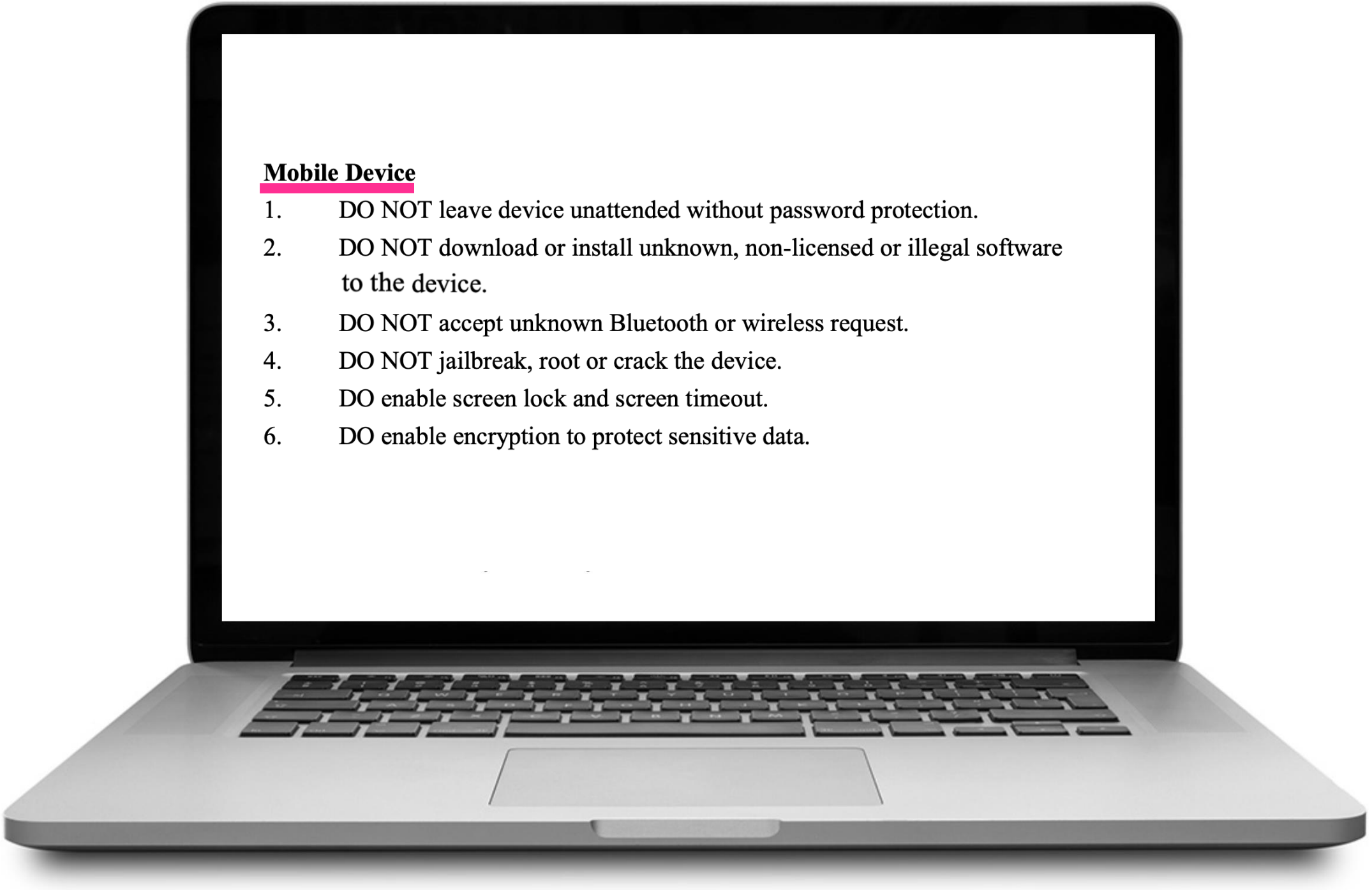
IT Security Training for New Staff (Induction Day)


仁安醫院
UNION HOSPITAL
Security Guidelines
Introduction
Unawareness of security issues may cause disclosure of confidential information, possibility of fraud, risk of computer abuse, etc. These guidelines are trying to increase the general awareness on computer security and provide advisory on using it. Users should get more IT security information to increase their general knowledge on how to use IT more efficiently and safely.


Guidelines
User ID & Password
1. DO NOT access to any systems unless you are authorized.
2. DO NOT disclose your user account and password.
3. DO NOT write down any of your user account or password and stick in open area.
4. DO NOT include your name or personal related words in the password.
5. DO NOT choose a used password as system will keep a history of 12 passwords
6. DO change your password regularly (e.g. every 120 days).
7. DO choose a password at least 8 characters long (mixing letters, numbers and symbols). e.g. G3o4%O5d6 !V which is combination of !§GoOd!··, !§3456!·· and !§%!··.
8. DO logoff systems when you leave the office.


Email systems
1. DO NOT open any unknown emails, such as spam mail.
2. DO NOT open attachments with extension .exe, .com.
3. DO save and scan all email attachments for viruses before opening them.
4. DO refer to E-mail Policy & Guidelines.
Internet Access
1. DO NOT access to Internet unless you are authorized.
2. DO NOT download any unknown programs from the Internet.
3. DO NOT trust any certificates from any unknown website during Internet browsing.
4. DO NOT access or browse any unethical websites, such as erotic, gambling & crack ware sites.
5. DO NOT disclose personal information to Internet Web sites.


Workstation
1. DO NOT leave PCs unattended without password protection.
2. DO NOT leave printout at printer unattended when printing sensitive documents.
3. DO NOT install or execute unknown software (especially downloaded from Internet).
4. DO NOT share any folder to others with unlimited access.
5. DO NOT use personal removable media such as external hard disk, USB drive, memory card, floppy disk, CD/DVD-ROM etc.
6. DO NOT store company data in public service provider (such as Google drive, Dropbox, SkyDrive, etc.).
7. DO use company provided PC for business only.


Mobile Device
1. DO NOT leave device unattended without password protection.
2. DO NOT download or install unknown, non-licensed or illegal software to the device.
3. DO NOT accept unknown Bluetooth or wireless request.
4. DO NOT jailbreak, root or crack the device.
5. DO enable screen lock and screen timeout.
6. DO enable encryption to protect sensitive data.

仁安醫院
UNION HOSPITAL

Biannual Personal Data Privacy Training Seminars

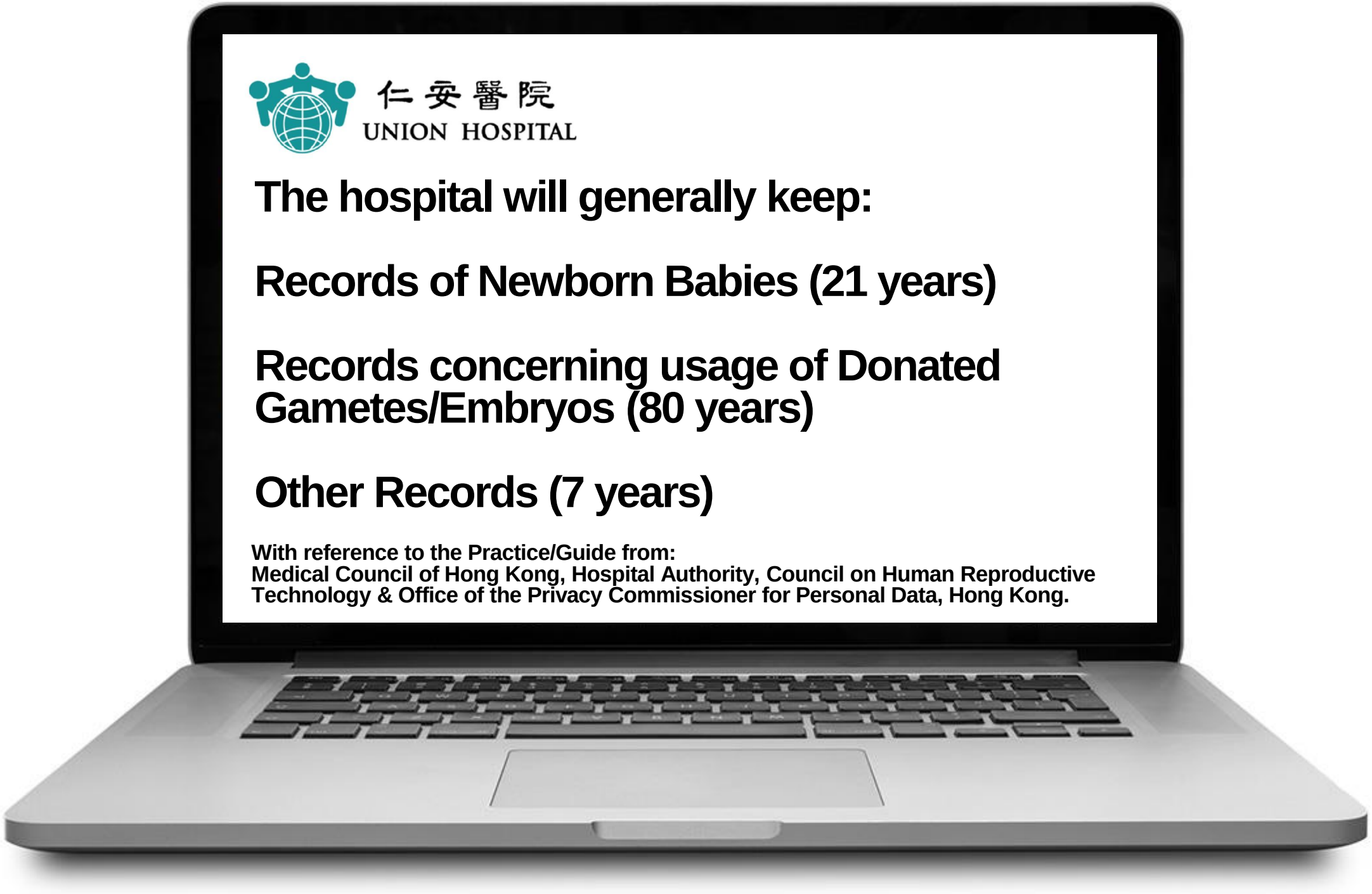
仁安醫院
UNION HOSPITAL

Log of All Access to Medical Records

仁安醫院
UNION HOSPITAL

Access Rights according to “Patient-under-care” & “Need-to-know” Basis


仁安醫院
UNION HOSPITAL
About Us
Services
Charges
Doctors
Health Info
News Room
Doctor's Corner
Location & Transportation
Contact Us
Privacy Policy Statement
Statement of Policy
Union Medical Centre Limited and its subsidiary, affiliated or related companies, including Union Hospital (collectively "we", "us" or "our") understand the importance of protecting the privacy, confidentiality and security of the personal information we hold by complying with the data protection principles and all relevant provisions under the Personal Data (Privacy) Ordinance.
It is important that you read this Privacy Policy Statement together with the applicable personal information collection statement of the relevant service, website, and/or mobile application provided by us. So that, you are fully aware of how and why we are using your personal data. This Privacy Policy Statement supplements other notices of us and is not intended to override them.
Find Union Good Doctors
By Doctor Name
By Specialty
View all >>
Service Booking & Enquiry
Submit


仁安醫院
UNION HOSPITAL
The hospital will generally keep:
Records of Newborn Babies (21 years)
Records concerning usage of Donated Gametes/Embryos (80 years)
Other Records (7 years)
With reference to the Practice/Guide from:
Medical Council of Hong Kong, Hospital Authority, Council on Human Reproductive Technology & Office of the Privacy Commissioner for Personal Data, Hong Kong.


Healthcare Cybersecurity

Healthcare Cyber Security Watch Pilot Program

Involved Parties	- Union Hospital & other 7 private hospitals/healthcare organisations - Hospital Authority - Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) - Microsoft Hong Kong & other cybersecurity companies
Objectives	- Situational Awareness of Emerging Attacks - Cyber Security Trend Report and News in Healthcare

Cyber Security Drill

Involved Parties	- Union Hospital - Hospital Authority - Hong Kong Police Force - Electronic Health Record Office
Objective	- Test the response time and coordination between different parties


Domain Name System (DNS) Firewalls and Anti-Malware Software


Access Control
Authorisation of Access
User Identification & Authentication
Audit Logging


Dataset Partitioning
Encryption of Personal Data
Backup & Recovery Drills
Conducting Vulnerability & Penetration Tests

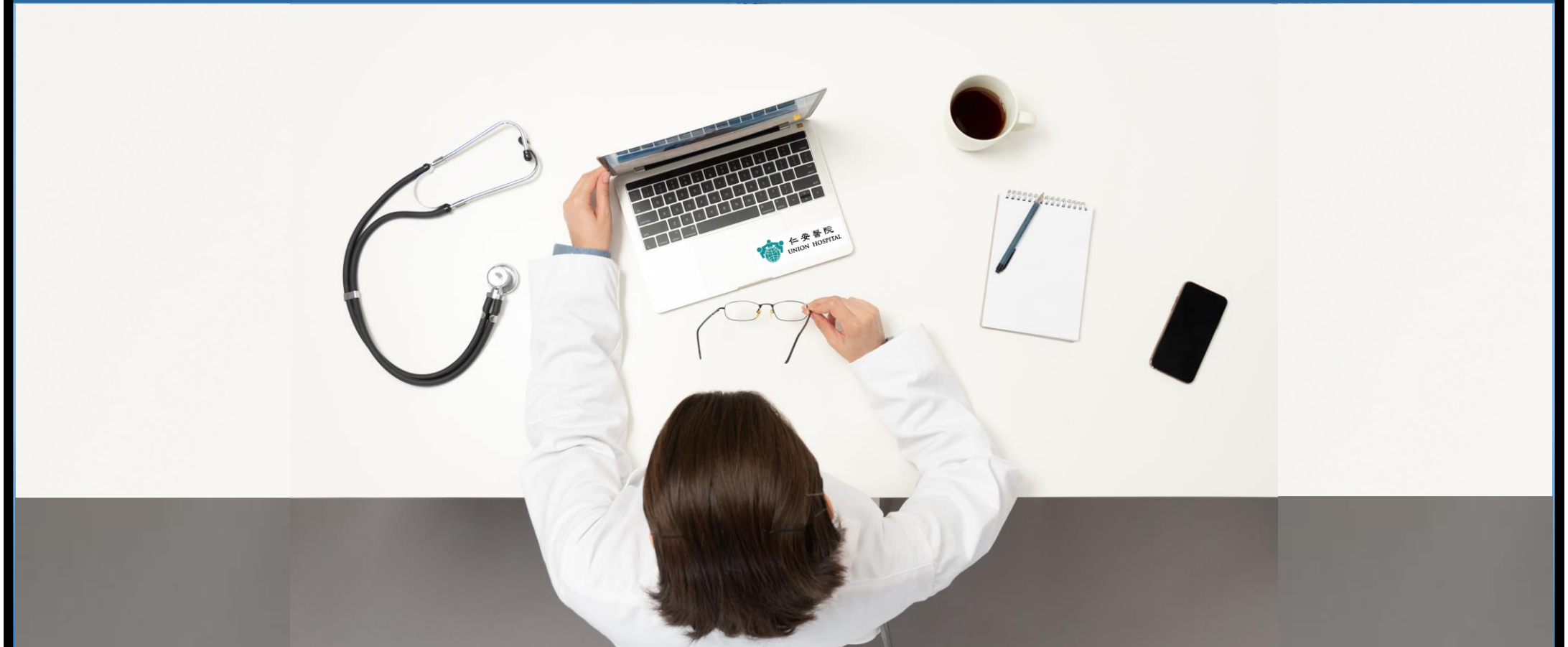
仁安醫院
UNION HOSPITAL

Telecommunication and Telemedicine Policy

1 Introduction

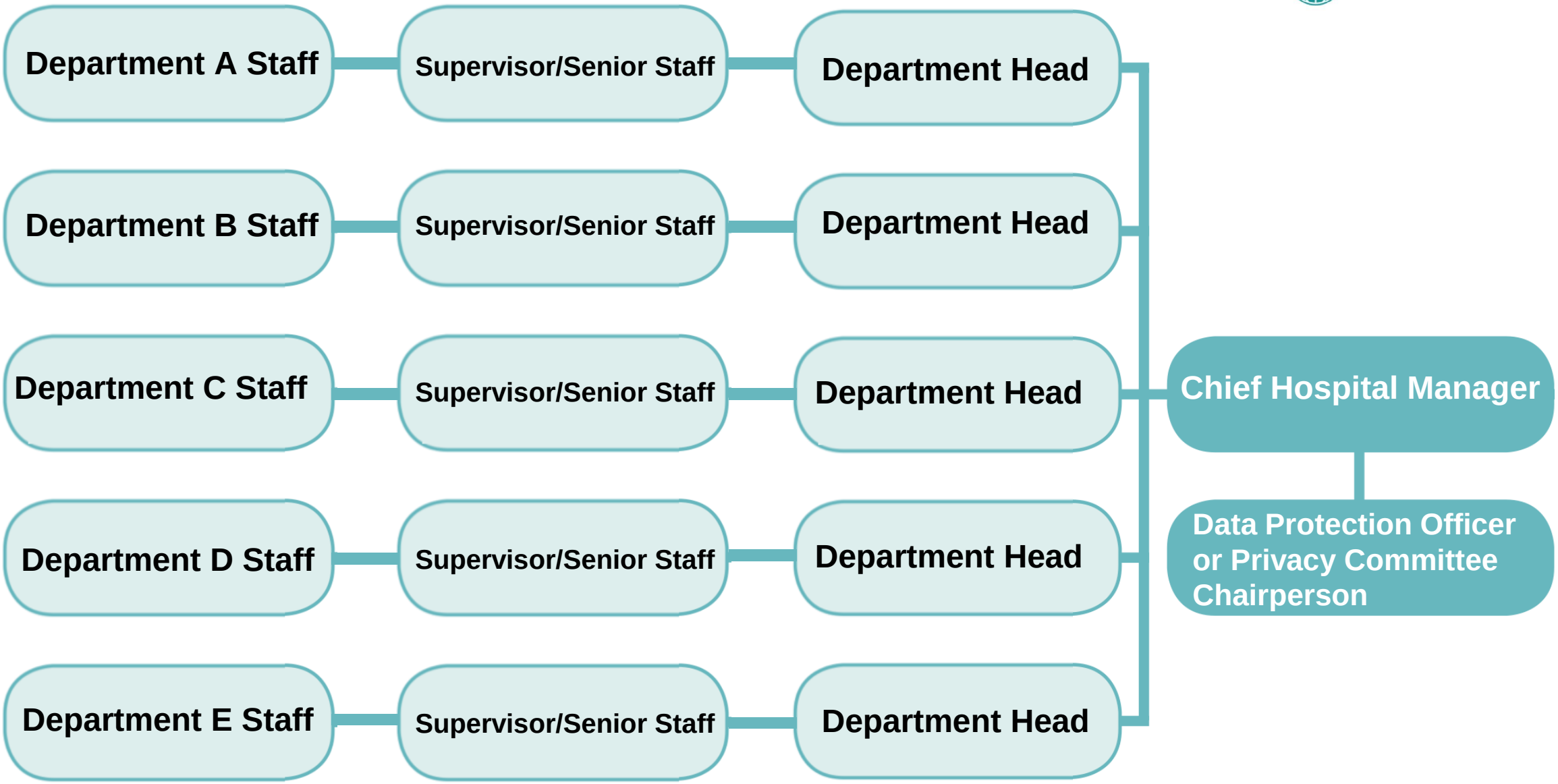
1.1 The advancements and continued development of medical and communications technology have had a profound impact on the practice of medicine and offer opportunities for improving the

Risks in Teleconsultation



Data Breach Reporting Mechanism

仁安醫院 UNION HOSPITAL



Union Hospital

Data Breach Notification Form

仁安醫院 UNION HOSPITAL

For further information, please refer to the Data Breach Notification Policy

I. Particulars of the person giving this notification (i.e. the data user)

(Under section 2(1) of the Personal Data (Privacy) Ordinance (the "Ordinance"), "data user", in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.)

Name: _____ | | | | **Dept:** _____ **Date:** _____

II. Details about the data breach

(Under section 2(1) of the Ordinance, "data subject", in relation to personal data, means the individual who is the subject of the data.)

Please provide the following information as specific as possible:

i) What personal data were concerned?

_____

_____

仁安醫院
UNION HOSPITAL

Data Breach Notification Policy

A. Statement of policy

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorized or accidental access, processing, erasure, loss or use. It may amount to a contravention of Data Protection Principle 4 – security of personal data of the Personal Data (Privacy) Ordinance.

In Union Hospital ("UH"), we are committed to protecting the privacy, confidentiality and security of the personal information we hold by complying with the requirements of Personal Data (Privacy) Ordinance with respect to the management of personal information. We are equally committed in ensuring that all our staff uphold these obligations.

All staff, who are involved in the handling and processing personal data collected by and originated from the UH must comply with this policy and to maintain vigilance in the protection of security and privacy

仁安醫院
UNION HOSPITAL

Standard Working Guideline SWG 0.1(5)
Guideline on Departmental Risk Registry

1. INTRODUCTION

1.1 Departmental Risk Registry is a documented repository for staff to identify, monitor and review risk at departmental level in a proactive and systematic manner. It is composed of 3 sections, including Risk Description, Risk Rating and Formulation of Action Plan.

1.2 Departmental Risk Registry is designed to capture risk from a bottom up approach where individual departments and units conduct periodic risk assessments to identify local risks. Information associated with these risks would be communicated upwards to management levels for an effective management of risk at both departmental and hospital-wide level.

2. PROCESS

INTRODUCTION

2.1 Departmental staff are required to **report risk(s)** and **update the progress of follow up action**, whenever necessary. Quick guide on Departmental Risk Registry is available in section 3.1-3.3.

2.2 The risk register is continuously monitored by the Risk Management Committee.

2.3 Risk registry data would be discussed in Management Review & Risk Prevention Meetings and Risk Management Committee Meetings (totally four times a year).

2.4 QAT would remind all departments to review and update the Departmental Risk Registry (as below) via email in January and July.

Layout of the Departmental Risk Registry

UNION HOSPITAL - DEPARTMENTAL RISK REGISTRY
Department: All

Details of using the Departmental Risk Registry is available in SWG 0.1(5) Guideline on Departmental Risk Registry

* Consequence Score	1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Major)	5 (Catastrophic)
# Likelihood Score	1 (Rare)	2 (Unlikely)	3 (Possible)	4 (Likely)	5 (Almost Certain)

General			Risk Description		Risk Rating					Action Plan					
			Reference: Risk Taxonomy		Reference: SWG 0.1 (3) Risk Registry Guideline					Reference: Category of Follow-up Action					
No	Dept.	Date of Risk Added	Risk Category	Brief Description of Risk	Type	Consequence Score*	Likelihood Score#	Total Risk Score	Risk Response Plan	Action Plan Category	Action Plan Sub-Category	Brief Description of Action Plan/ Progress	Target Completion Time	Date of Last Update	Status of Follow Up Action
Dr-XXX-00X (Dept.)		dd/mm/yyyy	Select from dropdown list	Please type	Select from dropdown list			Do not edit	Select from dropdown list	Select from dropdown list	Please type			dd/mm/yyyy	Select from dropdown list
			Choose...		Choose...	Choose...	Choose...	#VALUE!	Choose...	1 Choose...					Choose...
			Choose...		Choose...	Choose...	Choose...	#VALUE!	Choose...	1 Choose...					Choose...
			Choose...		Choose...	Choose...	Choose...	#VALUE!	Choose...	1 Choose...					Choose...

The Union Hospital Risk Management Framework

4. Risk Management Process

The 5-step Risk Management Process, including Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, and Risk Monitoring and Review together with the Risk Registry System is applied within the organisation.

4.1.Step 1 : Risk Identification

i) It is important to consider risks across different categories. These categories help identify and address potential hazards and threats effectively. While the specific categories may vary, here are some common risk categories:

1. Clinical and Surgical Risks: These risks involve potential errors or complications in clinical and surgical procedures that may impact patient safety and outcomes.

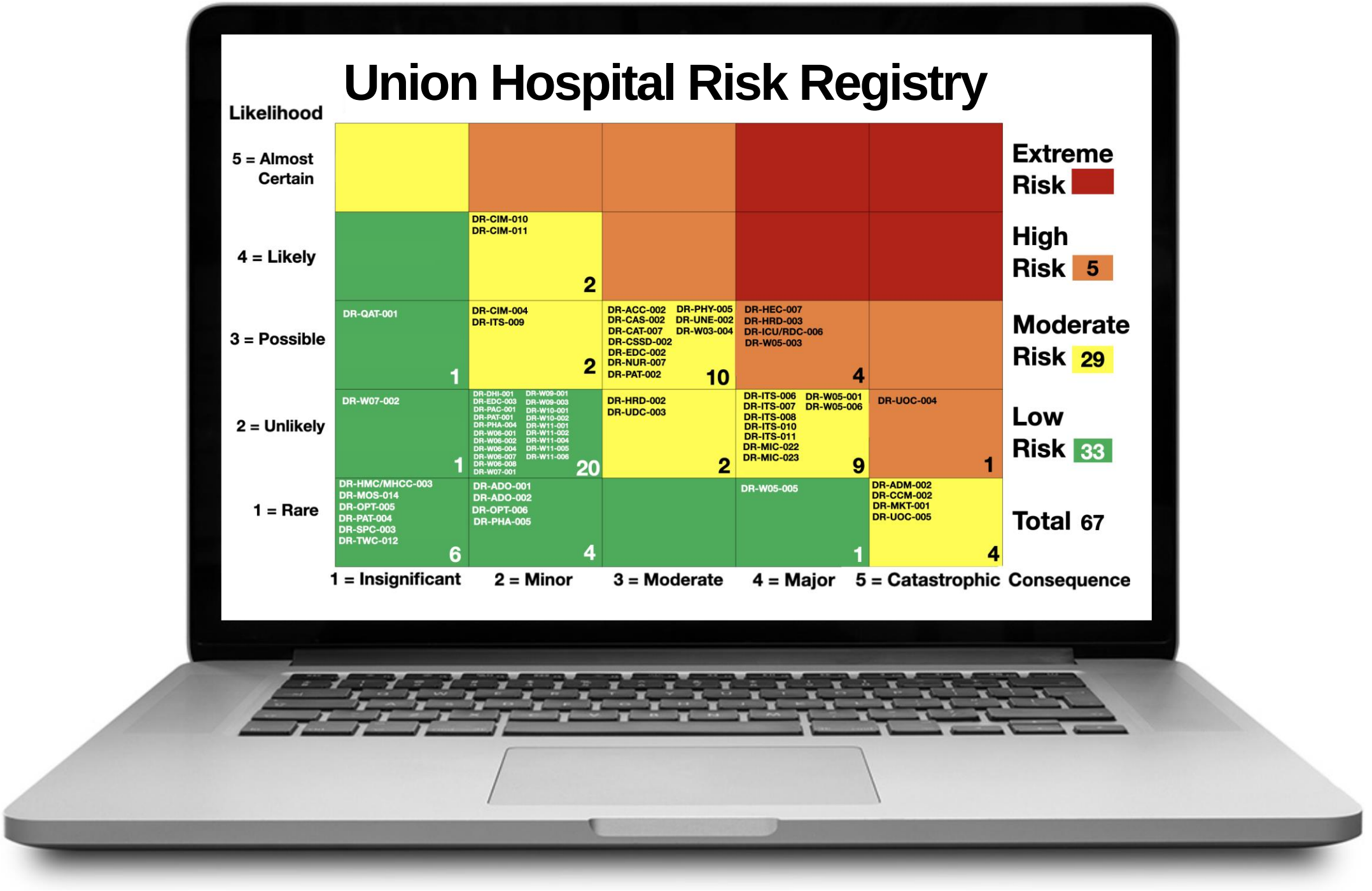
2. Patient Privacy and Data Security Risks: Risks related to breaches of patient privacy and data security, including unauthorised access to medical records or sensitive information.

3. Operational Risks: Risks associated with the day-to-day operations of the hospital, such as equipment failure, supply chain disruptions, or staffing issues.

4. Financial Risks: Risks related to financial management, including budgeting, billing, reimbursement, and financial fraud or mismanagement.

5. Legal and Regulatory Risks: Risks arising from non-compliance with applicable


Staff Risk Reporting Platform
員工風險通報平台由仁安醫院風險管理委員會成立，目的是為員工提供一個網上渠道以呈報院內風險，希望員工能夠以負責任及有效的方式表達意見。此平台所收集之個人資料及意見將會保密，並只用作醫院安全及風險管理之用途。
注意: 如同事需呈報特別事件/投訴/負評，請跟據SWG 0.1(2)c 處理特別事件/投訴/負評程序 呈報予管理層。
The Staff Risk Reporting Platform is prepared by the Risk Management Committee of Union Hospital to provide all staff with an online channel for reporting risk in the hospital. Staff are encouraged to voice out their concerns in a responsible and effective manner. All personal information and feedback would be treated in strict confidence and information collected would be used for hospital safety and risk management purposes.
NOTE: In case of special event, complaint or negative feedback, staff should report to the management according to SWG 0.1(2) Handling of Special Events / Complaint / Negative Feedbacks.
*必須填寫 Mandatory Field
*你的姓名 (Name):
*員工編號 (Staff No.):
*所屬部門 (Department):
*聯絡電話 (Contact Number):
*聯絡電郵 (Email):
*主風險類別 (Risk Category):
*次風險類別 (Risk Subcategory):
*內容 (Description):
送出(Send)
Launch on 20 November 2017
Intranet → Quality Management System → CQI & Risk Management


Union Hospital Risk Registry
Likelihood
5 = Almost Certain
4 = Likely
3 = Possible
2 = Unlikely
1 = Rare
DR-CIM-010
DR-CIM-011
2
DR-QAT-001
1
DR-CIM-004
DR-ITS-009
2
DR-ACC-002
DR-CAS-002
DR-CAT-007
DR-CSSD-002
DR-EDC-002
DR-NUR-007
DR-PAT-002
DR-PHY-005
DR-UNE-002
DR-W03-004
10
DR-HEC-007
DR-HRD-003
DR-ICU/RDC-006
DR-W05-003
4
DR-W07-002
1
DR-DHI-001
DR-EDC-003
DR-PAC-001
DR-PAT-001
DR-PHA-004
DR-W06-001
DR-W06-002
DR-W06-004
DR-W06-007
DR-W06-008
DR-W07-001
DR-W09-001
DR-W09-003
DR-W10-001
DR-W10-002
DR-W11-001
DR-W11-002
DR-W11-004
DR-W11-005
DR-W11-006
20
DR-HRD-002
DR-UDC-003
2
DR-ITS-006
DR-ITS-007
DR-ITS-008
DR-ITS-010
DR-ITS-011
DR-MIC-022
DR-MIC-023
DR-W05-001
DR-W05-006
9
DR-UOC-004
1
DR-HMC/MHCC-003
DR-MOS-014
DR-OPT-005
DR-PAT-004
DR-SPC-003
DR-TWC-012
6
DR-ADO-001
DR-ADO-002
DR-OPT-006
DR-PHA-005
4
DR-W05-005
1
DR-ADM-002
DR-CCM-002
DR-MKT-001
DR-UOC-005
4
1 = Insignificant
2 = Minor
3 = Moderate
4 = Major
5 = Catastrophic
Consequence
Extreme Risk
High Risk 5
Moderate Risk 29
Low Risk 33
Total 67

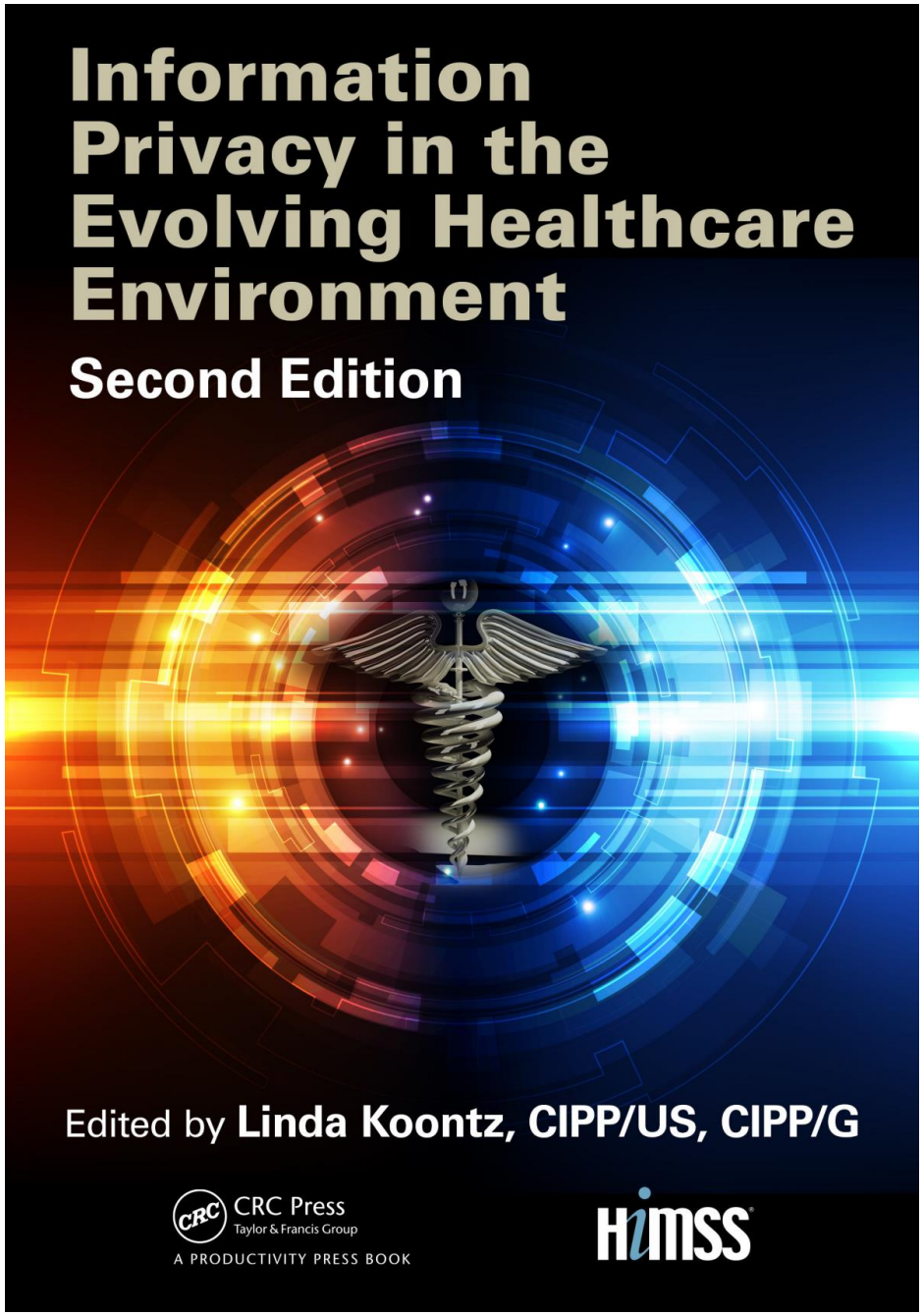
Risk Management Committee

Terms of Reference

- To oversee Risk Management Framework including the identification, assessment, analysis, monitoring, and mitigation of risks in order to ensure alignment with hospital objectives.
- To review and monitor hospital policies and any proposed changes to ensure that potential risks to patient safety, staff safety, smooth operation, and hospital reputation are being effectively managed and controlled.
- To ensure that the Risk Management Framework is in place with staff's good understanding and compliance against the relevant internal processes and policies.
- To provide recommendations and ensure that corrective or preventative measures are being taken to reduce, mitigate or eliminate risk re/occurrence.
- To review available data and analysis so as to provide regular update to the members of Management Review and Risk Prevention Meeting on a half yearly basis.
- To develop and maintain a comprehensive Risk Register System which will be reviewed at timely or at Management Review and Risk Prevention meeting on a half yearly basis. There will be generally 4 meetings concerning risk management in a year.
- To ensure all information relating to Risk Management policies are disseminated to relevant parties.

Helen Nissenbaum, Professor of Information Science:

"(Personal Data) Privacy is … a Right to the Appropriate Flow of Personal Information."



Reference: Linda Koontz, Information Privacy in the Evolving Healthcare Environment, 2nd edition (CRC Press, 2017), p. 18 (Kindle Edition).