epihc | ETHICAL PRINCIPLES IN HEALTH CARE™

In partnership with the
Government of Japan

Module 7 Summary

epihc.org

ETHICAL PRINCIPLE 7 – SAFEGUARDING PATIENT INFORMATION

THE WHY, THE HOW AND YOUR DUTY

SCENARIO

PRIVATE INFORMATION OF CELEBRITIES ACCESSED

LEGAL CASE

DATA BREACH OF PATIENT RECORDS

KEY LEARNINGS, CRITICAL DUTIES AND OBLIGATIONS

1. Continuously educate and sensitise all staff to data protection risks, particularly arising from receipt of emails.
2. Advise patients, staff, and other individuals if their data has been breached and shared.
3. Act honestly and responsibly, prohibiting practices which harm patients, and handle any actual or perceived threats or risks to patient, staff, and customer data with urgency, transparency, and sensitivity.
4. Maintain appropriate administrative, technical, and physical safeguards to ensure that:
   a. Organisational records, documents, and reports –physical, digital or electronic – are kept accurate, complete, and protected from tampering.
   b. Medical information is kept confidential.
   c. Information is protected from loss or misuse.
   d. Confidentiality of patient, staff and customer records is maintained in accordance with applicable legal and ethical standards.
   e. Staff refrain from discussing patients and their conditions in public areas.
   f. Data is not sold or monetised without the consent of those contributing to the data.

1. Understand the regulatory framework governing data protection.
2. Review governance structures, formal policies, and procedures which support the use and protection of data and align with the regulatory framework.
3. Evaluate gaps in governance processes and make recommendations on how to close these gaps in data protection and support best practice as per the WHO Data Principles,
4. Escalate areas of significant risk particularly in relation to data breach to the Board Risk Committee.
5. Develop protocols and procedures for cyber-attacks and data leaks.
6. Ensure that patient services subscribe to the highest standards of data protection mechanisms.
7. Consider how diverse stakeholders with different tasks and interests play a role in data breach types, facilitators, and impacts.
8. Consider the institutional factors that contribute to organisational noncompliance with data protection measures, and how regulators and healthcare organisation stakeholders can collectively address these factors.
9. Protect intellectual property, including trademarks, copyrights and patents, of vendors and other stakeholders.

YOUR DUTIES AND OBLIGATIONS

NOTES FOR MANAGERS

Following good practice is non-negotiable!

NOTES FOR SENIOR EXECUTIVES AND BOARD MEMBERS

Feigning ignorance is not a valid defence!