Introduction to Medical Information Security

Week 1 — Foundations of Medical Information Security

- Course: **IMI62-332 Medical Information Security**
- Focus: Concepts, risks, and controls in healthcare environments
- Today: Foundations, context, and case-based discussion

Learning Objectives (Week 1)

By the end of this session, students should be able to:

- Explain the **definition and purpose** of information security
- Describe the **CIA triad** and apply it to healthcare cases
- Discuss why **health data** is uniquely sensitive
- Identify **technical, administrative, and human** security components
- Analyse simple **case studies** using security concepts

Definition of Information Security

Information Security

- Protection of information to maintain:
  - **Confidentiality** – prevent unauthorised disclosure
  - **Integrity** – prevent unauthorised modification
  - **Availability** – ensure timely and reliable access
- Conceptual framework: **CIA Triad**
- In healthcare: supports **safe, continuous, and reliable care delivery**

Beyond the CIA Triad

Additional properties often considered:

- **Authenticity**
  - Assurance that users, devices, and data are genuine
  - Example: verifying physician identity before signing orders
- **Accountability / Non-repudiation**
  - Actions can be traced to responsible individuals or systems
  - Example: audit trails of who accessed which patient record and when

These properties support **clinical audit**, **legal evidence**, and **governance**.

Importance in the Healthcare Sector

- Health data = **highly sensitive personal information**
- Consequences of breaches:
  - **For patients**:
    - Discrimination, exclusion, social stigma
    - Psychological distress and loss of trust
  - **For organisations**:
    - Service disruption, delayed care, cancelled procedures
    - Financial loss, legal penalties, reputational damage

Real-World Threats to Healthcare

Common examples:

- **Ransomware attacks on hospitals**
  - Systems encrypted; EMR and PACS unavailable
  - Potential data exfiltration and blackmail
- **Unauthorised access to EMR systems**
  - Insider misuse (curiosity, fraud)
  - External attackers exploiting vulnerabilities

Real-World Threats to Healthcare

- **Insecure communication channels**
  - Patient data sent via personal email or consumer messaging apps

All of these impact **patient safety**, not only privacy.

Healthcare as a High-Risk Environment

Characteristics increasing cyber risk:

- Extensive digitalisation (EMR/EHR, PACS, LIS, HIS)
- 24/7 operation and low tolerance for downtime
- Legacy systems and medical devices with long lifespans
- Complex vendor ecosystem and interconnected networks

Result: **Attractive target** but often **under-resourced** in cybersecurity.

Components of Information Security

To achieve effective protection, three dimensions must work together:

1. **Technical measures**
2. **Administrative (organisational) measures**
3. **Human factors and organisational culture**

Weakness in any one dimension can compromise the others.

Technical Measures

Examples in healthcare settings:

- **Data encryption**
  - At rest: databases, backups, mobile devices
  - In transit: HTTPS/TLS, VPNs for remote access
- **Role-Based Access Control (RBAC)**
  - Permissions based on roles (physician, nurse, pharmacist, admin)
  - Application of **least privilege** principle

Technical Measures

- **Intrusion Detection/Prevention Systems (IDS/IPS)**
  - Monitoring for suspicious activities and attacks
  - Alerts for unusual logins, large data transfers, or scans

Administrative Measures

Organisational controls:

- **Security policies and procedures**
  - Password rules, acceptable use, incident reporting, backup policy
- **Risk assessment and risk management**
  - Identification of assets, threats, vulnerabilities, and impacts
  - Prioritisation of controls based on risk levels
- **Vendor and third-party management**
  - Contracts and agreements for systems handling health data
  - Clarification of responsibilities and minimum security requirements

Human Factors

People are central to both risk and defence:

- **Social engineering**
  - Phishing emails, fake IT calls, tailgating into secure areas
- **Human errors**
  - Misaddressed emails, lost devices, misconfigured access rights
- **Training and capacity building**
  - Regular awareness campaigns and simulations
  - Clear guidance and simple reporting channels

> Technology alone is insufficient; **behaviour and culture** are critical.

Key Standards and Frameworks (Overview)

- **ISO/IEC 27001**
  - International standard for Information Security Management Systems (ISMS)
  - Emphasises a **risk-based and continuous improvement** approach
- **NIST Cybersecurity Framework (CSF)**
  - Five core functions: **Identify, Protect, Detect, Respond, Recover**
  - Widely used as a practical structure for cybersecurity activities

Health Data Regulations and Standards

- **HIPAA (USA)**
  - Privacy and Security Rules for protecting health information (PHI)
- **PDPA (Thailand)**
  - Personal Data Protection Act; health data as **sensitive personal data**
  - Defines duties of data controllers/processors and rights of data subjects
- **HL7 and FHIR**
  - Standards for **interoperable exchange** of health information
  - Crucial for secure, accurate data sharing between systems

These frameworks shape **legal obligations** and **technical design**.

Distinct Characteristics of Health Data

Health data differs from many other data types:

- **High sensitivity** (diagnoses, genetics, mental health, reproductive health)
- **Long-term retention** for clinical, legal, and research purposes
- **Multiple formats**:
    - Text, codes, lab results, images, signals, video, audio
- **Intensive data sharing**
    - Across departments and organisations (referrals, insurers, national systems)

Result: **Security requirements are more stringent and complex.**

Secondary Use of Health Data

Beyond direct patient care:

- **Research and clinical studies**
- **Quality improvement and benchmarking**
- **Public health surveillance and policy**
- **AI and data analytics**

Security and privacy issues:

- De-identification and re-identification risks
- Governance of data reuse and data sharing agreements
- Transparency and patient expectations

Health Data Flow in a Hospital

Typical flow:

Patient
→ Outpatient / Emergency registration and examination
→ **EMR/EHR** documentation
→ **Laboratory / Radiology** requests and results
→ **Specialty clinics** and consultations
→ **Billing and financial systems**
→ **Health network systems** (HIE, insurers, registries)

Each step introduces **interfaces** and **new risk points**.

Security Considerations Along the Data Flow

- **Registration and front desk**
  - Risk of overheard conversations, visible screens, misplaced forms
- **EMR/EHR systems**
  - Risk of shared accounts, weak authentication, excessive privileges
- **Laboratory and Radiology systems (LIS, PACS)**
  - Legacy platforms, unencrypted archives, limited patching
- **Billing and financial systems**
  - Combined exposure of financial and medical data
- **External exchanges (HIE, insurers, ministries)**
  - Complex trust relationships and cross-organizational responsibilities

Week 1 Summary (Practical)

Key takeaways:

- Recognise the **types of health data** and their clinical importance.
- Understand how security incidents can harm both **patients** and **organisations**.
- Begin to apply CIA and basic security concepts to **realistic scenarios**.
- Appreciate the role of **standards and regulations** in shaping practice.

These foundations will support deeper topics in subsequent weeks.

Further Reading (Optional)

Students may consult:

- Introductory chapters on information security (CIA, risk management) from cybersecurity textbooks
- Public reports of recent **hospital ransomware incidents**
- National or institutional guidelines on **health data protection**
- Short introductions to **ISO/IEC 27001**, **NIST CSF**, or local data protection regulations

Thank You

Week 1 Completed

Questions and discussion are welcome.