SHEng
SMART HEALTHCARE ENGINEERING
2023-1-RO01-KA220-HED-000159985

Co-funded by
the European Union

HOSPITAL INFORMATION MANAGEMENT SYSTEMS

Class Content Material

This document is part of a training materials collection developed within the Erasmus+ project “Smart healthcare engineering”, SHEng, project No. 2023-1-RO01-KA220-HED-000159985.

The collection is intended for engineering students and professionals working in the healthcare sector. It covers technical subjects relevant to hospital infrastructure, equipment, materials and support services, helping readers understand how engineering contributes to safe patient care and the reliable operation of healthcare facilities.

These materials support classroom teaching and independent study. They should be used alongside the project handbook and the presentations, courses and other learning resources available on the project website. Each document addresses a specific subject, while the collection provides a broader understanding of the responsibilities and practical challenges of healthcare engineering.

The content is educational. Its application in practice requires consideration of the conditions of each healthcare facility, the applicable standards and the instructions provided by equipment manufacturers.

Project website: www.smarthealtheng.com

SHEng
SMART HEALTHCARE ENGINEERING

Transilvania University of Brasov
ULPGC Universidad de Las Palmas de Gran Canaria
MANISA CELAL BAYAR ÜNİVERSİTESİ
Servicio Canario de Salud
SPITALUL MUNICIPAL SĂCELE
Co-funded by the European Union

HOSPITAL INFORMATION MANAGEMENT SYSTEMS

Modules, standards, security and operation

Okan Çöllü, Manisa, Hafsa Sultan Celal Bayar University Hospital, Türkiye

Introduction

A hospital information management system (HIMS) collects, stores, processes and exchanges the clinical, administrative and financial data of a hospital. It supports registration, orders, clinical records, medication, laboratory and imaging requests, billing, supplies and management reporting. These functions have different users and different risks. A registration clerk needs speed and accurate identity data, a physician needs a complete and readable record, and a manager needs reliable, aggregated figures.

1. System fundamentals

What a HIMS is

A HIMS is a combination of software modules, databases, interfaces, hardware and work procedures. Some modules are built by one supplier, and some are specialised systems from other suppliers, connected through interfaces. Its purpose is to make the right information available to the right person at the right time. Installing software does not by itself achieve this, because the result depends on how staff use it and on the quality of the data they enter.

The main modules are shown in fig.1. A central layer keeps the patient identity and the shared data, while departmental modules read and write through it. Some departments may still use their own

systems for specialised work, so the interfaces between modules are as important as the modules themselves. A weakness in one interface can appear to the user as a fault of the whole system.

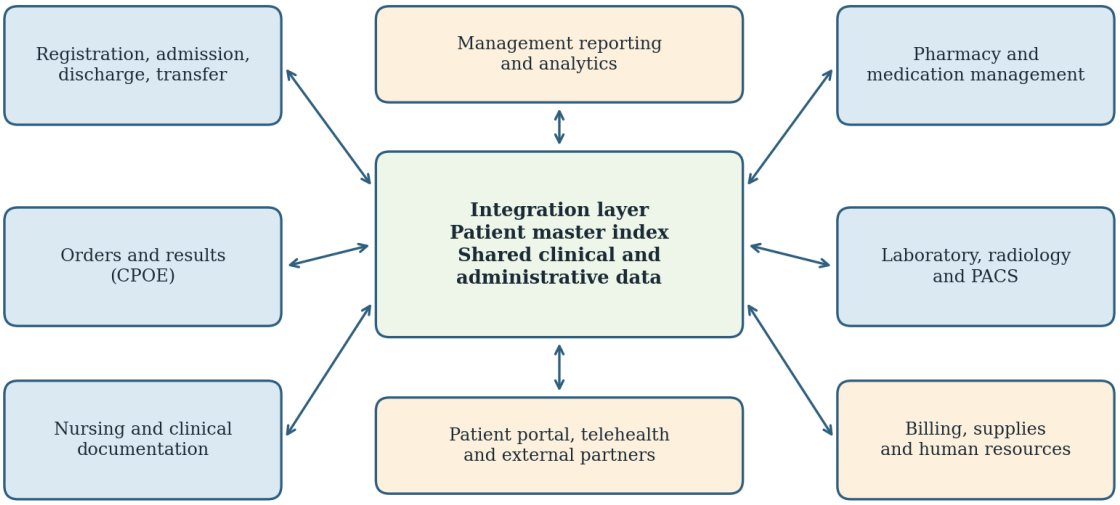

Figure 1. Main modules and data flows of a HIMS

Terms that should not be confused

Table 1. Terms used around hospital information systems

Term	Meaning	Hospital example
HIS / HIMS	Whole set of systems that run a hospital	Registration, orders, billing and reporting together.
EHR	Longitudinal record of a patient, shared across providers	Record that follows a patient between hospitals.
EMR	Record kept inside one organisation	Hospital chart used on the wards.
ADT	Admission, discharge and transfer function	Bed and location of an inpatient.
CPOE	Computerised entry of clinical orders	Physician orders a drug or blood test.
MPI	Master patient index linking identities	Detects the same patient registered twice.

The terms overlap in daily use. A tender or a contract should state which functions are included, because a product sold as an EHR may not contain billing or inventory, and a financial system may not contain a clinical record.

2. Core modules and functions

Table 2. Common modules and their purpose

Module	Main function	Typical use
Registration and ADT	Identify patients and track admissions	Creates the patient record and bed allocation.
Order entry (CPOE)	Send clinical requests to services	Laboratory, imaging and drug orders.
Clinical documentation	Record history, notes and care plans	Ward rounds and nursing observations.
Pharmacy	Manage prescribing, dispensing and stock	Medication administration record.
Laboratory and imaging	Receive requests and return results	Results appear in the patient chart.
Billing and finance	Prepare charges and claims	Invoices for patients and payers.
Supplies and staff	Manage inventory, rosters and assets	Stock levels and duty schedules.

The ADT function is the backbone of the system, since almost every other module depends on knowing who the patient is and where the patient is. An error in identity or location spreads to orders, results and bills. Functional models such as ISO/HL7 10781 describe what an electronic record system should be able to do and can support the preparation of requirements [1].

Medication safety and decision support

Computerised order entry can reduce transcription errors and make orders legible, but it does not make prescribing safe by itself. Medication safety improves when order entry, pharmacy verification and administration at the bedside are connected, for example through barcode checking of patient and drug. Decision support rules such as allergy and interaction checks help only if they are accurate and appropriately selective. Too many low value alerts lead staff to override them, so the alert rules need regular review with clinicians.

3. Standards and interoperability

Messages, documents and terminologies

Data exchange between modules and between organisations relies on standards. HL7 version 2 messages are still widely used for admission, order and result messages inside hospitals, while HL7 FHIR provides a web-based way to exchange resources and is increasingly used for new interfaces

and patient applications [2]. Clinical documents can be exchanged in structured formats such as CDA. IHE profiles describe how these standards should be combined for tasks such as patient identity matching and document sharing [3].

Table 3. Standards used in hospital information systems

Standard	Role	What it does not do
HL7 v2	Messages between hospital systems	Does not fix local differences in how fields are used.
HL7 FHIR	Resources and web interfaces	Does not guarantee that two systems use the same codes.
IHE profiles	Defined use of standards for a workflow	Must still be tested in each installation.
ICD, SNOMED CT, LOINC	Codes for diagnoses, concepts and tests	A code in the record is not proof of correct coding.

Syntactic interoperability means that a message can be read, while semantic interoperability means that both sides understand it in the same way. A message that is accepted without error may still carry a laboratory code that the receiving system maps wrongly. Terminology mapping therefore needs clinical review and a named owner [4].

Patient identity is the most sensitive element of the exchange. Duplicate records, records merged by mistake and temporary identities for unidentified patients are common risks. A master patient index with clear matching rules and a controlled merge procedure is needed, and every merge should leave an audit trail.

4. Architecture, availability and continuity

Architecture models

A hospital may choose a single integrated suite or a set of best-of-breed systems connected through an integration engine. An integrated suite simplifies data sharing and support, while a best-of-breed approach can fit a specialised department better but increases interface work. The hosting may be on premises, in a hospital data centre, in a cloud service or in a hybrid form. No model removes the responsibility of the hospital for lawful processing, access control and recovery of the data. Location of the data, the cost of retrieving it and the procedure for leaving a supplier should be defined in the contract.

Availability and recovery

Availability is often quoted as a percentage, and small differences matter. An availability of 99.9% allows about 8.8 hours of unplanned stoppage per year, while 99.99% allows about 53 minutes. Such a figure should state which services are included and whether planned maintenance is counted. The recovery point objective, which describes how much data may be lost, and the recovery time objective, which describes how long recovery may take, should be agreed with the clinical departments.

A backup is not the same as a replica. A replica can copy an error, a deletion or an encrypted file to the second site, so at least one independent copy should be kept and restoration should be tested, not assumed. Performance is a separate matter. A value expressed in transactions per second does not describe how fast a screen opens for a physician during morning rounds, and load tests should therefore use realistic workflows.

Downtime procedures

Every ward needs a documented procedure for the period when the system is not available. It should cover access to a read-only copy of key patient data, paper forms for orders and medication, the identification of patients without system labels and the process for entering the data afterwards. The procedure should be practised, because paper routines that have not been used for years are difficult to follow in an emergency.

5. Data quality and problem analysis

Reports and decisions are only as reliable as the data entered at the point of care. Typical sources of poor data are free-text entry where coded entry is needed, copying of old notes, and workarounds created because a screen does not match the real workflow. Mandatory fields may also be filled with default values to move on, which gives complete but incorrect records.

Table 4. What an observed problem may mean

Observation	Possible explanation	What to check
Same patient has two records	Registration without search or failed matching	Search routine, matching rules and merge log.
Result missing from the chart	Interface error or wrong code mapping	Interface queue, message log and code table.

Observation	Possible explanation	What to check
Drug order not seen by pharmacy	Order status or routing rule	Order status, routing rule and user role.
Screens slow during rounds	Database load, network or workstation	Server load, network path and local device.
Claims rejected by the payer	Missing diagnosis or procedure code	Coding at discharge and billing rules.

Do not correct the record before documenting the problem. Note the original values, the time and the user, and use an authorised correction procedure that keeps the history. An error that reached a clinical decision should be handled as a patient safety incident, and the fix should address the cause, not only the individual entry.

6. Applications in healthcare facilities

Outpatient, inpatient and emergency care

In outpatient care the system supports appointments, referral, consultation records and follow-up. In inpatient care it supports bed management, orders, nursing observations and discharge planning. The emergency department needs rapid registration, triage and a clear overview of waiting patients, so the same module cannot simply be copied from the wards.

Theatre, laboratory, pharmacy and imaging

Operating theatres use scheduling, consent and instrument or implant records. Laboratory, pharmacy and imaging systems handle requests and results and are often separate products linked to the HIMS. The quality of these links decides whether the clinician sees a single record or a set of unrelated screens.

Management, patient access and analytics

Management reporting uses the same data for bed occupancy, waiting times, costs and quality indicators. An indicator is reliable only when its definition and the source fields are fixed. Patient portals and telehealth tools give patients access to appointments and results, but they require strong identity checks. Analytical and artificial intelligence tools should be validated for the local population, and their output should not replace clinical judgement.

7. Security, privacy and regulation

Health data belong to a special category of personal data and need strong protection. Security must be part of the design, not an added step. Table 5 lists common measures and their limits.

Table 5. Common security measures and their limits

Measure	Purpose	Limitation
Role-based access	Limit data to what the role requires	Roles must be reviewed when staff change.
Emergency access	Allow urgent access with a recorded reason	Needs review of every use.
Audit trail	Record who viewed or changed data	Useful only if the logs are reviewed.
Encryption and backup	Protect data in transit, storage and recovery	Does not stop misuse by an authorised account.
Patching and monitoring	Reduce known vulnerabilities	Some systems depend on supplier approval.

Most breaches involve people and procedures as well as technology, for example shared passwords or access that is not removed when staff leave. Regular training, review of access rights and a tested incident response plan are therefore part of the control set. Guidance such as ISO 27799 helps to apply information security management to health data [5].

Data protection law such as the GDPR and national equivalents requires a lawful basis, data minimisation, defined retention and rights of access for patients [6]. Decision support or analysis software that is intended for diagnosis or treatment decisions may qualify as medical device software, for example under the EU Medical Device Regulation [7]. The manufacturer's intended purpose and the software lifecycle standard IEC 62304 are relevant in that case [8]. Where the HIMS is linked to medical devices on the hospital network, risk management according to IEC 80001-1 should be applied [9].

8. Implementation, maintenance and continuity

Specification and selection

A specification should describe functions, interfaces, performance, security and service levels, not only a product name. Requirements should come from physicians, nurses, administrative staff, IT and information security staff. A demonstration with the hospital's own scenarios gives better

evidence than a general presentation. Configuration is usually preferable to custom programming, since custom changes need to be maintained and tested after every upgrade.

Migration, training and go-live

Migration from an old system needs a plan for patient identity, active episodes and the history that must remain visible. Counts and sample checks should be compared before and after, and the old system should not be switched off until the result has been verified. Training should follow real roles and workflows. A phased introduction by department limits risk, while a single go-live date is simpler to coordinate but demands strong support during the first weeks.

Operation and improvement

After go-live, change control, regular testing of interfaces, monitoring of queues and storage, and a clear service agreement keep the system reliable. Feedback from users should be collected and reviewed, because poor usability leads to workarounds that reduce data quality and safety. The benefits claimed in the business case should be measured against agreed indicators.

References and standards

[1] ISO/HL7 10781. Electronic health record system functional model.
[2] HL7 International. HL7 Version 2 messaging standard, HL7 FHIR and HL7 CDA.
[3] IHE International. IHE IT Infrastructure and Patient Care Coordination Technical Frameworks (including patient identity cross-referencing and document sharing).
[4] WHO International Classification of Diseases (ICD); SNOMED International, SNOMED CT; Regenstrief Institute, LOINC.
[5] ISO 27799. Health informatics: information security management in health using ISO/IEC 27002.
[6] Regulation (EU) 2016/679 (General Data Protection Regulation).
[7] Regulation (EU) 2017/745 on medical devices.
[8] IEC 62304. Medical device software: software life cycle processes.
[9] IEC 80001-1. Application of risk management for IT-networks incorporating medical devices.

Acknowledgments

The content was supported by the project “Smart Healthcare Engineering (SHEng)”, Grant Agreement No. 2023-1-RO01-KA220-HED-000159985, co-funded by the Erasmus+ programme of the European Union. Results, views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Transilvania University of Brasov

ULPGC Universidad de Las Palmas de Gran Canaria

MANİSA CELAL BAYAR ÜNİVERSİTESİ

Servicio Canario de Salud

SPITALUL MUNICIPAL SĂCELE

Co-funded by the European Union