Welcome to the Laboratory Information Management Systems Module
Module Objectives

At the end of this module, participants will be able to:

- Describe important elements of an information management system;
- Discuss guidelines on standards, policies and best practice of Information Management;
- Explain things to consider when developing a manual, paper-based information system;
- Describe the advantages and disadvantages of a computerized information management system;
- Discuss IT governance and best practice;
- Discuss IT standards and security.
“You manage a laboratory for a 300 bed hospital and the administrator has just notified you that funds are available for the purchase of a computerised laboratory information system.”

How do you assess the relevancy of such a system for your laboratory?
Information Management

Establish processes for managing data

- Computer-based
- Patient Information
- Patient Sample details
- Specimen Processing
- Result entries

- Paper-based

- Accessible
- Accurate
- Timely
- Secure
- Confidential
- Private

Source: WHO – Training Toolkit
Information Management Elements

- Unique identifiers for samples & patients
- Standardised request forms
- Logs, worksheets
- Checking processes
- Data protection
- Confidential
- Effective reporting systems
- Effective communication

Important elements
Patient identifiers — Patients who are hospitalised must have a unique patient identifier, often bracelets are used. It is advisable that this unique patient identifier is used for the duration of the hospital stay.

Sample identifiers — Unique identifiers must be allocated to patient samples, so they can be tracked throughout the laboratory.

Forms: -- Standardise the test form—the form should indicate all information that needs to be provided when ordering and submitting a test request, and in the design there must be sufficient space for recording the information; make sure that it is completed correctly.

Logs and worksheets must be kept. Recording data at the time of arrival of the sample in the laboratory are kept in a log book, while a worksheet is used to record which patient samples are being tested during a certain procedure. In a paper-based system, this will be a written record, usually in a bound book. For an electronic system, logs and worksheets may be generated from the computer. One must decide as to what information should be recorded.
<table>
<thead>
<tr>
<th>Processes:</th>
<th>Errors can occur at any time when handling data. Put processes in place as precaution and protection against errors at these points. Implement formal checking processes to ensure the accuracy of data recording and transmission of handwritten or keyed information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection:</td>
<td>Protect against loss of data. For paper-based systems, use safe materials for recording and storing the records properly. For computerized systems, regular backup processes are required.</td>
</tr>
<tr>
<td>Confidentiality:</td>
<td>Protect patient’s privacy by implementing security measures to guard the confidentiality of laboratory data. Policies and procedures to assure confidentiality of patient information must be put in place and this is the responsibility of the laboratory director.</td>
</tr>
<tr>
<td>Reporting systems:</td>
<td>The test result, or the report is the final product of the laboratory. The test result must be issued timeously. It must also be accurate, legible, and easily understood. It should be verified and signed by the appropriate laboratory staff.</td>
</tr>
<tr>
<td>Communication:</td>
<td>When planning for paper-based or computer-based information systems, consider the need for a good communication system that enables a laboratory to connect both internally and externally.</td>
</tr>
</tbody>
</table>
Common problems

- Computer systems incompatible
- Data incomplete
- ID (patient/sample) insufficient
- Forms inadequate
- Data organized poorly
- Archiving poor
- Transmission errors
Developing a paper-based system

Staff need to be informed that when using a paper system, the following points are important:

- All data entry must be complete. Handwritten logs must be checked.
- Emphasize to employees the importance of legibility.
- If issuing handwritten reports, the laboratory must always make a copy for its files or archives. Not having an exact copy of the report can lead to later problems, if errors in transcription occur.
Storing paper-based materials

Goals:
- Find results
- Trace samples
- Evaluate occurrences

Useful rules:
- Keep everything for a designated time
- Ensure easy access
- Use a logical system for filing
- Number in chronological order
Storing paper-based materials (continued…)

Paper is brittle, and susceptible to water, fire, humidity, and vermin (rodents and insects). Use a storage area that will protect against these elements as much as possible.
A computerised system for laboratory data is known as a laboratory information management system and is referred to by the acronym LIMS or LIS.

A well planned and installed LIMS brings accuracy and accessibility to the flow of samples and data in the clinical laboratory.
Laboratory Information Management System

Advantages of LIMS

- Integrate with other sites
- Error Reduction
- QC
- Financial management
- Data retrieval options
- Access control
- Detailed, legible reports
- Track, analyse trends
- Track reports
The Use of LIMS in Disease Management

- **Pre Analytics**
  - Request Forms
  - Patient demographics
  - Patient History
  - Test

- **Post Analysis**
  - Patient demographics
  - Test
  - Patient Results

- **Tools to be used**
  - Analysers
  - Stats from the LIS

- **Lab Resources**
  - Pathologists, Scientists, Medical Technologists
Process: Path of Workflow
Referrals between Laboratories
Laboratory Connectivity

Reference Lab

Network Link

TB Lab

HIV Lab

Malaria Lab
A Data Centre is a facility or centralized repository used for storage and management of Data.

This includes computer and server operations, data entry, data security, data quality control and management of services and applications used for data processing.

Management of Data Centre requires a number of tools, policies and strategies to create and maintain.
IT Governance and Best Practice

- ITIL®
- COBIT5 (audited tool)
- Prince 2
- King III
ITIL v3 Life Cycle
Key issues facing many of today’s senior Business Managers and IT Managers in Service Management includes:

- IT and business strategic planning;
- Integrating and aligning IT and business goals;
- Implementing continual improvement;
- Measuring IT organization effectiveness and efficiency.
Organizations that use IT depend on IT to be successful. ITIL gives guiding processes to ensure that the business’s success can be achieved ….

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement
Service Strategy
For an organisation to be successful, the services provided must be perceived by the customer to deliver sufficient value in the form of outcomes that the customer wants to achieve.

Service Design
The design of appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements.

Service Transition
The role of Service Transition is to deliver services that are required by the business into operational use.
ITIL® Service Management Cycle (continued...)

Service Operation

Is to deliver agreed levels of service to users and customers, and to manage the applications, technology and infrastructure that support delivery of the services.

Continual Improvement

Continual Service Improvement (CSI) is concerned with maintaining value for customers through the continual evaluation and improvement of the quality of services and the overall maturity of the ITSM service lifecycle and underlying processes.
COBIT5 Principles

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a single integrated framework
4. Enabling an holistic approach
5. Separating Governance from Management
COBIT5 Principles (continued…)

1. Principles, Policies and Frameworks

2. Processes

3. Organizational Structures

4. Culture, Ethics and Behaviour

5. Information

6. Services, Infrastructure & Applications

7. People, Skills & Competencies

Resources
IT Governance is the ability of senior management to direct, measure and evaluate the use of IT resources to achieve organisations strategic goals.

Cobit5 provides guidelines on adopting a formal approach to IT governance by setting out standard procedures and processes to be implemented by IT departments in order to improve service delivery to customers and Risk management.
Cobit Framework is set out of 34 high level processes, grouped into 4 domains that cover all aspects of IT.

**Measurement scales 0-5**

0 - Non-Existent  
1 - Initial/ Ad-hoc  
2 - Repeatable but intuitive  
3 - Defined Process  
4 - Managed And Measurable  
5 - Optimised
Data protection and security are critical components of routine pathology practice because laboratories are legally required to securely store and transmit electronic patient data.

Computer equipment, data, information, and computer services should be protected from unintended or unauthorized access.

Data should be made available to clients for years after release for research and legal purposes, dictated by law or governance.
All electronic systems or devices that play a role in generating, capturing, storing, or modifying patient data require security review. This includes LIS hardware and software as well as devices that can access LIS data (i.e., mobile devices such as tablet computers or smart phones) or interfaced devices such as instruments or point of care testing devices.

Laboratories should establish audit programs to ensure that access to health information systems is appropriate and has not been compromised.
Written policies are required to cover the mechanisms available to provide individuals with access to information systems.

Policies and procedures for terminating access, such as when staff leaves the health-care organization need to be implemented.

In addition, security awareness training should be provided to all staff members. Initial general training should be reinforced through periodic security reminders.
A major requirement of laboratory computer systems used to manage patient information is their reliability.

Laboratories should have procedures for both planned and unplanned system outages (i.e., down-time) which should address how the laboratory should function during the outage and the sequence in which all impacted software in the laboratory (LIS, middleware, instrument software, etc.) are brought back online once the outage has been resolved.
For planned outages (i.e., down-time that occurs to perform system maintenance or an upgrade), the procedure should define the sequence as well as the process for shutting systems down. For unplanned events, procedures should assign responsibility for determination of the cause of the outage to defined individuals as well as the process and persons responsible for performing disaster recovery.

Down-time procedures should be logged /documented should specify the laboratory's response based on the type of system outage (e.g., LIS, instrument, network etc.) can be updated annually as systems or risks change.
Any unplanned outage can result in data loss, it is critically important for the laboratory to develop robust data protection mechanisms that minimize loss and help speed up the recovery process.

Different Backup mechanisms can be used
Summary

- System for managing both incoming and outgoing data.
- May be paper-based or computer-based.
- Both require a similar framework, including unique identifiers, forms, logs and worksheets.
- Cost is a major factor in using a computer-based system.
- A good information management system will:
  - Ensure all data—the final product of the laboratory—is well managed
  - Consider all the ways laboratory data will be used when planning a system
  - Assure the accessibility, accuracy, timeliness, and security of data
  - Ensure confidentiality and privacy of patient information
Disease management is made easy through the use of IT LIS.

Data can be accessed from a central storage centers.

Data in the LIS can be used for survey statistics.

Disease Hot spots or problem areas can be identified using patient results.

The results can be used in anonymity through the use of Unique Identifiers.

Historic data can be referred to, for future management of pandemics.

Security in Data centers and Lab Networks should be trusted to restrict use to only authorised users.
References

- WHO: Quality Management Toolkit
- ISO 15189:2012: Quality management in the clinical laboratory
- Guidance for Laboratory Quality Manuals (Ontario Laboratory Accreditation Division)
- ITIL_V3_Study_Guide (Taruu LLC)

Links

http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/
Wrap Up for Module 5

Participants are now able to:

- Describe important elements of an information management system;
- Discuss guidelines on standards, policies and best practice of Information Management;
- Explain things to consider when developing a manual, paper-based information system;
- Describe the advantages and disadvantages of a computerized information management system;
- Discuss IT governance and best practice;
- Discuss IT standards and security.
Questions