MODULE 15 | HOSPITAL INFORMATION SYSTEMS, RECORDS AND DATA

Managing Hospital Information Systems and Digital Workflows

59

LECTURE

Practical hospital governance in Punjab, Pakistan

Keep information available, accurate and protected.
Make digital work support safe patient care.

AUTHOR

Dr Qurban Hussain Khan

Edition 1.0 | 5 October 2026

SELF-STUDY PDF

A digital system is part of hospital operations

The Medical Superintendent (MS) needs enough understanding to ask the right questions, assign responsibility and protect care.

- Know which services depend on each system.
- Check authority, access and clinical safety before use.
- Prepare for outages and security incidents.
- Review evidence before accepting a system or a report.

OFFICIAL SOURCE

A principle tied to a named law, standard or official guidance.

WORKING METHOD

A practical control or teaching format to adapt to the authorised system.

TEACHING CASE

An invented hospital example, used to practise applying the correct process.

Study output

A system register, an access-control review and a tested plan for one critical service.

Module 15 | Presentation 1 of 3. Allow 45-60 minutes with exercises. All explanations are on the pages; check the cited sources before live use.

Three connected responsibilities

A working computer does not by itself establish a complete record or a reliable management figure.

Lecture	Main subject	Practical output
59	Hospital systems and digital workflows.	System register and service-continuity plan.
60	Medical records and lawful disclosure.	Record-control and disclosure checks.
61	Data quality and management reporting.	Verified measures and an action dashboard.

Study the systems, the patient record and the management report as related parts of one service.

WORKING METHOD | Illustrative material is identified in the text.

Separate requirements from useful guidance

Use the exact instrument, scope and current institutional order when making an official decision.

Source	How to use it
Law and official rules	Identify the provision, who it applies to and any conditions or later notifications.
PHC hospital standards	Check the applicable category and the evidence required for the relevant standard.
Institutional directions	Use approved responsibilities, security arrangements and operating procedures.
International guidance	Use it to improve a working method; do not present it as a Punjab legal requirement.

Software access, a vendor statement or an online approval button does not itself confer statutory or financial powers.

Sources: **I1**: IMS standards | **I4**: section 16 | **I7**: scope

Understand the main system names

Hospitals may combine these functions or run separate systems. Identify the actual local arrangement.

Term	Plain meaning
HMIS or HIMS	Hospital information management system: connects clinical and administrative work.
EMR	Electronic medical record: the patient’s clinical record in electronic form.
LIS and PACS	Laboratory information system; picture archiving and communication system for imaging.
e-FOAS	Electronic filing and office automation system: official files, notes and correspondence.

PITB descriptions illustrate these functions. They do not establish that every hospital has identical software.

Sources: **I2**: clinical and administrative modules | **I3**: e-filing functions

Name an owner for each decision

Suggested allocation. Confirm the actual institutional powers and appointment orders.

Role	Accountability to define
Institutional head / MS	Service priorities, resources, unresolved risks and escalation to the competent authority.
Clinical and records leads	Safe clinical workflow, record content, patient identity and authorised disclosure.
IT and security leads	Technical operation, security monitoring, access administration and recovery.
Finance, procurement and vendor	Lawful purchase, contract evidence, support and deliverables within assigned roles.

A vendor can provide technical support. The hospital still needs named officers for its own decisions.

WORKING METHOD | Illustrative material is identified in the text.

Create one current system register

A suggested register for each application and its important connections.

01 Service

What work depends on it, and who owns that work?

02 Information

Which patient, staff, financial or other records does it hold?

03 Location

Where are the system and its backup copies hosted?

04 Support

Who supports it, under which contract and hours?

05 Connections

Which devices or other systems send or receive data?

06 Recovery

Who can restore it, and when was this tested?

Include small departmental databases and spreadsheets when they support important decisions or hold sensitive records.

WORKING METHOD | Illustrative material is identified in the text.

Follow one patient journey through the system

Suggested exercise for clinical, nursing, records, laboratory, pharmacy and IT representatives.

1	**Register**	Create or find the correct patient record and identify the current encounter.
2	**Provide care**	Document assessment, orders, medicines and procedures under the correct patient.
3	**Act on results**	Route results to a responsible clinical team and check urgent results are acted upon.
4	**Close the encounter**	Complete discharge or transfer information and preserve access for authorised follow-up.

For each step, ask what happens if the screen, printer, network or receiving service is unavailable.

WORKING METHOD | Illustrative material is identified in the text.

Control patient identity before copying information

PHC IMS standard 28 addresses a unique patient record identifier and identifiable, timed entries.

At registration

- Use the hospital’s approved identifiers and search for an existing record before creating another.
- For an unidentified emergency patient, use the approved temporary-identity process and arrange later reconciliation.

When a mismatch appears

- Stop an unsafe transfer of information. Ask the authorised team to verify the person and the affected encounters.
- Keep a traceable correction. Do not merge records merely because names or phone numbers match.

Do not let an unresolved administrative identifier delay immediate clinical assessment and emergency care.

Sources: **I1**: standard 28

Keep codes and lists under control

Master data means the approved lists used throughout the system. These are suggested controls.

List	Error to prevent
Medicines and units	Confusing medicine strength, dose unit, form or route.
Tests and results	Wrong test code, specimen type, unit or reference information.
Locations and services	A ward, clinic or bed appearing under different codes in different reports.
Users and roles	Old staff accounts or inappropriate permissions remaining active.

Record who requested, checked and approved each change. Test affected screens, labels and reports before release.

WORKING METHOD | Illustrative material is identified in the text.

Test the connection between two systems

An interface is the connection that transfers information between systems. Suggested acceptance checks:

1	**Match identity**	Confirm patient, encounter, specimen and order identifiers remain correct.
2	**Match meaning**	Check codes, units, dates, status and corrected results in both systems.
3	**Test failure**	Try a delayed message, duplicate, rejected message and temporary connection loss.
4	**Confirm action**	Show who detects failed transfers and who receives and acts on urgent results.

A message marked “sent” is not evidence that the clinical team reviewed or acted on its content.

WORKING METHOD | Illustrative material is identified in the text.

Check the physical service behind the screen

Suggested joint review with IT, engineering and the department using the system.

01 Power

Test approved backup power for the essential equipment.

02 Network

Identify weak points and the support contact for failures.

03 Workstations

Provide usable, supported devices in the actual work areas.

04 Printing

Check safe labels, forms, consumables and printer cover.

05 Environment

Protect servers and equipment from heat, water and intrusion.

06 Support

Provide an escalation route during nights and holidays.

A software contract cannot compensate for an unplanned loss of power or an unusable clinical workstation.

Write requirements before choosing a product

Suggested content for the authorised procurement process; the procurement rules remain separately applicable.

Requirement	State a testable outcome
Clinical work	Which steps, safety checks and reports the system must support.
Operational capacity	Expected concurrent users, locations and response under realistic load.
Information control	Required access, correction, audit trail and approved reporting functions.
Continuity and exit	Recovery evidence, data export, transition help and usable records after contract end.

Ask staff who perform the work to review the specification. Keep requirements clear enough to test fairly.

WORKING METHOD | Illustrative material is identified in the text.

Make the contract usable during a problem

Suggested contract questions for legal, procurement, clinical and technical review.

Issue	What must be clear
Data and access	Hospital control, permitted vendor use, confidentiality and authorised support access.
Service levels	Support hours, incident categories, response and restoration commitments, and evidence.
Costs and changes	Licences, interfaces, maintenance, training, upgrades and change-approval charges.
Exit and handover	Readable export, file formats, audit history, migration help and controlled vendor-copy disposal.

Record the approved acceptance conditions and payment milestones. Access to records must not depend on an undocumented promise.

WORKING METHOD | Illustrative material is identified in the text.

Accept the system on evidence

Suggested acceptance checks, using authorised test data and the agreed specification.

01 Clinical paths

Registration, orders, medicines, results and discharge work.

02 Permissions

Each role can do its permitted tasks and no more.

03 Failure paths

Errors, outages, duplicate entries and recovery are handled.

04 Connections

Devices and interfaces exchange correct information.

05 Migration

Transferred records reconcile and remain understandable.

06 Sign-off

Users and technical officers record results and open defects.

User acceptance testing means intended users check the system against agreed needs. Keep actual results, not only a completion certificate.

WORKING METHOD | Illustrative material is identified in the text.

Start live use through a controlled decision

Suggested approach. The scope and timing must reflect patient risk and local capacity.

1	**Prepare**	Resolve critical defects, train users and confirm accounts, equipment and support.
2	**Try a limited scope**	Use an approved pilot with clear clinical oversight and measurable checks.
3	**Decide to proceed**	Review evidence, unresolved risks and a workable fallback before extending use.
4	**Watch early work**	Track safety concerns, delays and staff problems; assign and close corrective actions.

Define which record is authoritative during any paper-and-electronic transition. Reconcile differences promptly.

WORKING METHOD | Illustrative material is identified in the text.

Treat each major change as a service decision

Suggested change-control record for updates, new interfaces and important configuration changes.

1	**Describe**	State the request, reason, affected services and consequences of doing nothing.
2	**Assess**	Check clinical, record, security and financial effects with the responsible owners.
3	**Test and approve**	Record tests, competent approval, timing, user communication and rollback plan.
4	**Check after release**	Verify the intended result and review errors; retain the change history.

An urgent repair still needs an authorised decision and a traceable record, followed by a prompt review.

WORKING METHOD | Illustrative material is identified in the text.

Give each person the right access

PKCERT guidance supports individual credentials and stronger authentication. A suggested hospital access process follows.

Before access is issued

- The line manager confirms identity, role, location, dates and tasks; the system owner approves suitable permissions.
- IT issues an individual account. Multi-factor authentication adds a further check, such as a verified device, where required by the approved security design.

When the role changes

- Review access after transfer, promotion, rotation or leave arrangements. End unneeded access promptly when the person leaves.
- Provide an approved urgent-access route for clinical need. Record why it was used and review the event.

Shared clinical accounts make it difficult to establish who entered or changed a patient’s record.

Sources: **I5**: password and access guidance

Control powerful and remote accounts

Suggested access register for IT administrators and vendors.

Control	Evidence to keep
Named purpose	The approved task, system and officer responsible for the access.
Limited access	Only needed privileges, a defined period and an approved connection method.
Oversight	Logs of relevant activity and an officer who can review unusual changes.
Closure	Confirmation that temporary access ended and the requested work was checked.

A service contract is not unlimited permission for a vendor to browse patient records or copy the database.

WORKING METHOD | Illustrative material is identified in the text.

Make routine security part of daily work

PKCERT’s public-sector handbook addresses official channels, approved devices and prompt reporting.

What staff need to know

- Use approved accounts and devices. Verify an unusual request through a known official contact before acting.
- Report suspicious messages, lost devices or unexpected system behaviour through the published support route.

What management should arrange

- Give staff a short, tested contact list and a way to obtain help during clinical duty.
- Ask IT to report overdue repairs and unsupported equipment with a service-risk decision, owner and date.

Training should use safe examples and practical reporting exercises. Do not put real passwords or patient records in teaching material.

Sources: **I5**: email, devices and incident awareness

Use audit logs to investigate facts

An audit log records specified system events. The detail available depends on system design and configuration.

Useful questions

- Which account viewed, created, changed, printed or exported the affected information? What time and record were involved?
- Are clock settings consistent, logs protected and authorised reviewers able to retrieve the required period?

Limits and safeguards

- A username is evidence about an account, not conclusive proof of the individual actor. Check other evidence.
- Restrict log access, preserve relevant records and use the proper inquiry process before reaching a finding.

Set log coverage and retention through approved risk, legal and operational requirements. Lecture 60 addresses record retention and holds.

WORKING METHOD | Illustrative material is identified in the text.

A backup must be capable of restoration

A backup is a recovery copy. Recovery planning must include people, equipment, applications and dependencies.

Ask for a recovery demonstration

- Which record set was recovered, from which point in time, and how long did restoration take?
- Could authorised users find the right patient, open results and continue the necessary workflow?

Check the arrangement

- Keep protected recovery copies separate from the live system’s main failure risks and test restoration.
- Record failed tests and corrective action. A successful backup message alone does not prove recovery will work.

Backup retention and the legal retention of the medical record are different decisions; coordinate both.

Sources: **I5**: data security | **I8**: recovery and exercises

Two recovery targets answer different questions

Invented planning example. RPO and RTO are approved planning targets, not statutory hospital limits.

RPO: data gap	Recovery point objective: the maximum data period the plan can tolerate losing. A 1-hour target requires a recovery design able to meet that gap.
RTO: service time	Recovery time objective: the planned time allowed to restore the defined service. Specify when timing starts and what counts as restored.
Observed test	An outage starts at 10:00. The usable recovery copy is from 08:00; the defined service returns at 13:00. Data gap = 2 hours; restoration = 3 hours.
Decision	Against illustrative targets of 1 hour RPO and 2 hours RTO, both targets were missed. Review the causes, clinical fallback and recovery design.

Targets must follow the service’s clinical needs and resources. A target in a contract is not evidence of achieved recovery.

Sources: **I8**: contingency-planning concepts

Use a prepared plan when systems stop

Suggested downtime process; clinical leaders decide the safe response for each affected service.

1	**Declare and contact**	Record the failure time, scope and incident lead; contact clinical, IT and duty-management teams.
2	**Continue safely**	Use approved paper forms, identifiers and essential service priorities with suitable clinical oversight.
3	**Keep results moving**	Assign a reliable route for urgent orders and results, including confirmation of receipt.
4	**Track the work**	Keep a controlled list of encounters, medicines, tests and other transactions needing later reconciliation.

If essential care cannot be delivered safely, escalate to the authorised clinical and operational response, including transfer arrangements where needed.

WORKING METHOD | Illustrative material is identified in the text.

Recover the service and reconcile the records

Suggested return-to-service checks after technical restoration.

1	**Verify readiness**	IT confirms technical recovery; clinical teams test the essential workflow.
2	**Agree the restart**	Name the authority, restart time and instructions for stopping temporary processes.
3	**Reconcile safely**	Match paper and electronic records; check pending results, medicine administration and duplicate orders.
4	**Review the event**	Identify harm, delay and missing information; assign corrective actions and update the plan.

Retain original downtime records as required. Do not make a late entry appear to have been entered at the original event time.

WORKING METHOD | Illustrative material is identified in the text.

Respond to a suspected cyber incident

Suggested hospital response. A technical incident may also be a patient-safety and information incident.

1	**Protect patients**	Activate the relevant clinical fallback and identify any risk to urgent services.
2	**Escalate immediately**	Use the approved IT/security and management contacts; record what was observed and when.
3	**Preserve evidence**	Let authorised specialists direct containment and evidence capture. Avoid unplanned wiping or alteration.
4	**Coordinate decisions**	Keep a timed action log, required reports, approved communications and a checked recovery plan.

Use the applicable official reporting route and directions. Do not wait for a full investigation before making a required initial report.

WORKING METHOD | Illustrative material is identified in the text.

Know the CERT reporting route in advance

CERT means Computer Emergency Response Team. Apply the rule’s scope and current official directions.

What the Rules state

- Rule 24 provides for designated points of contact. Rule 25(2) requires a functional entity to report initially within one hour to its Sectoral CERT and National CERT.
- The trigger is identification by its CSIRT, CERT or IT department. The initial report uses the best available estimate, followed by updates.

What the hospital should settle

- Confirm its applicable route, named contact, backup contact and current reporting instructions before an incident.
- Rule 25(1) also provides a direct National CERT route for affected persons or organisations outside a Sectoral CERT. Escalate internally at once.

CSIRT means Computer Security Incident Response Team. Do not apply this deadline indiscriminately to every complaint about privacy.

Sources: **I6**: rules 24-26

Make an electronic file a complete official case

PITB describes e-FOAS functions for files, notes and correspondence. Use the workflow authorised for your institution.

1	**Register**	Record the incoming item, receipt date, reference and correct subject or file.
2	**Prepare**	State the issue, facts, applicable authority, options and precise decision requested.
3	**Route and decide**	Attach the necessary evidence and send to the competent officers through the authorised sequence.
4	**Issue and follow up**	Preserve the approved version, signature or authentication, dispatch evidence and action due.

A file shown as “forwarded” has not necessarily been decided. Track the actual decision and its implementation.

Sources: **I3**: e-FOAS functions

Electronic form has legal conditions

The Electronic Transactions Ordinance 2002 addresses the legal recognition of electronic records and signatures.

Recognition and reliability

- Sections 3-6 address electronic form, writing, original form and retention, subject to the stated conditions on accessibility and integrity.
- Sections 7-9 address electronic signatures and proof. A pasted picture of a signature is not an automatic answer to every authentication requirement.

Public-authority workflow

- Section 16 concerns dealings with public authorities, including prescribed formats and processes; it does not create an unrestricted right to demand electronic acceptance.
- Use the authorised signing and filing method. Check competence, complete attachments and a retrievable final record.

Digitising a document does not create authority to approve its subject or automatically permit destruction of the paper original.

Sources: **I4**: sections 3-9 and 16

Approve new storage and AI tools before use

Cloud storage uses remotely hosted resources. AI means artificial intelligence; its output still needs responsible human review.

Before placing hospital data

- Ask who can access it, where it will be held, what the provider may use it for and how it can be returned.
- Obtain the applicable security, legal, procurement and institutional approvals. Use test or non-confidential material for demonstrations.

Before relying on an output

- Check accuracy, source and suitability. Identify the officer responsible for the decision or clinical action.
- Do not submit identifiable patient records to an unapproved public tool. A useful result does not establish lawful disclosure.

Treat draft legislation as a draft. Use enacted instruments, applicable directions and professional confidentiality obligations.

Sources: **I5**: approved platforms and oversight | **I9**: legislation register

Ask for a small system-performance report

Suggested measures. Define the period, scope and source before comparing results.

Measure	Management question
Service interruption	How long was essential work unavailable, and which patients or services were affected?
Unresolved safety defects	Which system problems could cause harm, and who owns the corrective action?
Access exceptions	Which overdue removals or unusual privileged uses need a decision?
Recovery and support	Did restoration tests pass, and are serious support cases being closed properly?

Lecture 61 explains data quality and dashboards. A green status box without supporting evidence is weak assurance.

WORKING METHOD | Illustrative material is identified in the text.

Organise the first month of review

Suggested sequence for an MS taking charge. These are working periods, not legal deadlines.

1	**First week**	Identify critical systems, owners, access contacts and the clinical fallback arrangements.
2	**Second week**	Review a patient workflow, one official file and the most serious unresolved defects.
3	**Third week**	Observe an authorised recovery or downtime exercise; review accounts and vendor access.
4	**Fourth week**	Present a short risk-and-action report with costs, owners, dates and decisions needed.

NIST’s six functions offer a useful review structure: Govern, Identify, Protect, Detect, Respond and Recover.

Sources: **I7**: six functions

TEACHING CASE

The laboratory screen fails during a busy shift

All people, events and hospital details in this teaching example are invented. They do not describe an actual hospital event.

What happens	The clinical screen stops receiving new laboratory results. The laboratory can still produce results locally.
Immediate risk	Several urgent results need review. Staff begin sending photographs of reports through personal messaging accounts.
Technical request	The vendor asks for a shared administrator password and a full copy of the patient database.
Management choice	The duty officer needs to continue safe result delivery, obtain technical help and preserve records of the outage.

Which immediate actions protect patients, and which proposed shortcuts need to be stopped or replaced?

TEACHING CASE | Illustrative material is identified in the text.

TEACHING CASE

A reasoned response to the laboratory outage

Suggested answer to the invented case; adapt the clinical escalation to the actual situation.

1	**Assign clinical follow-up**	Name the responsible teams and use the approved urgent-result route with confirmation.
2	**Use controlled records**	Track pending results and recipients. Replace unauthorised sharing with an approved fallback.
3	**Arrange limited support**	Approve named, time-limited technical access and only the data needed for the authorised task.
4	**Reconcile and review**	After recovery, check results, acknowledgements and duplicate messages; retain the incident record.

A technical outage requires a coordinated service response. It does not authorise unrestricted copying of patient information.

TEACHING CASE | Illustrative material is identified in the text.

Three decisions for the institutional head

Write your answer and the reason before turning to the next page.

1. Ready for payment?

The vendor shows a login screen and asks for final acceptance. Recovery and interface tests remain incomplete.

What evidence is needed before acceptance?

2. Recovery targets

An outage starts at 12:00. The usable data copy is from 11:30. Service returns at 14:30. Targets: 1-hour RPO; 2-hour RTO.

Which target is met, and which is missed?

3. Digital authority

An officer has an approval button but lacks the required delegated spending power.

Can the button provide the missing authority?

Give the reason, name the responsible decision-maker and identify the record that should be retained.

Answers and reasons

Use the evidence, the calculation and the cited source.

1. Acceptance needs the agreed evidence

Check completed tests against the contract, unresolved defects, clinical and technical sign-off and the competent acceptance decision. A login demonstration does not establish completion.

2. One target met; one target missed

Data gap = 30 minutes, within the 1-hour RPO. Service restoration = 2 hours 30 minutes, exceeding the 2-hour RTO by 30 minutes. Review actual clinical effects and the recovery gap.

3. Software permission is insufficient

The authorised officer must decide under the applicable delegation and process. Correct the system permissions and retain the proper approval trail; do not treat a button as a delegation order.

The exercise targets are invented. Live decisions require the current authority, service needs and approved procedure.

Produce a practical system-control file

Use a non-confidential real case or the invented examples in this lecture.

1. System register

List five important systems, their service owners, support routes and main dependencies.

2. One live workflow

Map a patient or official-file process. Identify three risks and the control needed for each.

3. Continuity review

Review one authorised recovery or downtime test and record the gaps, owners and actions.

Review with the clinical, records, IT and security leads. Present unresolved decisions to the competent authority.

Use non-confidential examples for teaching. Store operational details and sensitive records only in approved systems.

WORKING METHOD | Illustrative material is identified in the text.

Six questions before relying on a system

A short management review to use alongside the applicable rules and institutional procedures.

01 Purpose

Which essential service and decision does it support?

02 Authority

Who owns the process and may approve its actions?

03 Safety

Have the identity, workflow and failure risks been tested?

04 Access

Can only authorised people perform the relevant tasks?

05 Continuity

Can the hospital continue and recover with usable records?

06 Evidence

Can the stated result be checked against a reliable record?

Next: Lecture 60 examines the patient record, confidentiality, retention and lawful disclosure.

WORKING METHOD | Illustrative material is identified in the text.

Sources and continued use | 1

Select a source title or its official-source link to open the document.

I1

Minimum Service Delivery Standards for Hospitals 2024

Punjab Healthcare Commission Category I hospital manual. IMS standards 28-30 cover patient records, continuity, confidentiality and review. Apply the relevant hospital category and current directions.

Punjab Healthcare Commission | **Official source**

I2

Electronic Medical Record and Hospital Information Management System

PITB describes a PKLI-HPTC implementation and its clinical and administrative modules. This is an example of system scope, not proof that every Punjab hospital uses the same system.

Punjab Information Technology Board | **Official source**

I3

Punjab e-FOAS inauguration, 27 December 2023

Official description of e-filing functions and rollout intentions. Verify the hospital’s present connection, approved workflow and applicable departmental instructions.

Punjab Information Technology Board | **Official source**

Educational material by Dr Qurban Hussain Khan. Source editions are stated; verify later amendments and applicable institutional orders before live use.

Sources and continued use | 2

Select a source title or its official-source link to open the document.

I4

Electronic Transactions Ordinance 2002

Sections 3-9 concern recognition, writing, originals, retention and signatures. Section 16 concerns dealings with public authorities. Electronic records must meet the applicable conditions.

Ministry of Law and Justice, Pakistan Code | **Official source**

I5

National Cybersecurity Handbook 2026-27

Official public-sector guidance on accounts, devices, approved storage and reporting. Hospital checklists in this lecture are original working examples; apply current departmental security directions.

Pakistan National CERT; official FBR copy | **Official source** | **PKCERT publication page**

I6

Computer Emergency Response Team Rules 2023

Gazette of 3 October 2023. Rules 24-26 address contacts, reporting and directions. Rule 25(2) specifies functional entities and the reporting trigger; confirm the applicable route and current notifications.

Government of Pakistan; official PKCERT copy | **Official source**

Educational material by Dr Qurban Hussain Khan. Source editions are stated; verify later amendments and applicable institutional orders before live use.

Sources and continued use | 3

Select a source title or its official-source link to open the document.

I7

NIST Cybersecurity Framework 2.0, 2024

International risk-management guidance: Govern, Identify, Protect, Detect, Respond and Recover. Useful for organising questions and responsibilities; it is not a Punjab statutory certification.

US National Institute of Standards and Technology | **Official source**

I8

Contingency Planning Guide, SP 800-34 Revision 1

NIST guide, 2010, for US federal information systems. Used here for recovery planning concepts and testing. Hospital targets and procedures are teaching examples, not Pakistani legal limits.

US National Institute of Standards and Technology | **Official source**

I9

Ministry of IT and Telecommunication: legislation register

Distinguishes approved instruments from drafts. The May 2023 personal data protection bill is listed as a draft in the material checked for this edition; do not cite a bill as an enacted Act.

Ministry of Information Technology and Telecommunication | **Official source**

Educational material by Dr Qurban Hussain Khan. Source editions are stated; verify later amendments and applicable institutional orders before live use.