Module 2: eHealth Data Privacy, Security, Legal Frameworks & Ethics

DigHealth –

Micro-credentials in digital health for Ethiopia and Somalia

Proj. Ref. Num. 101179425

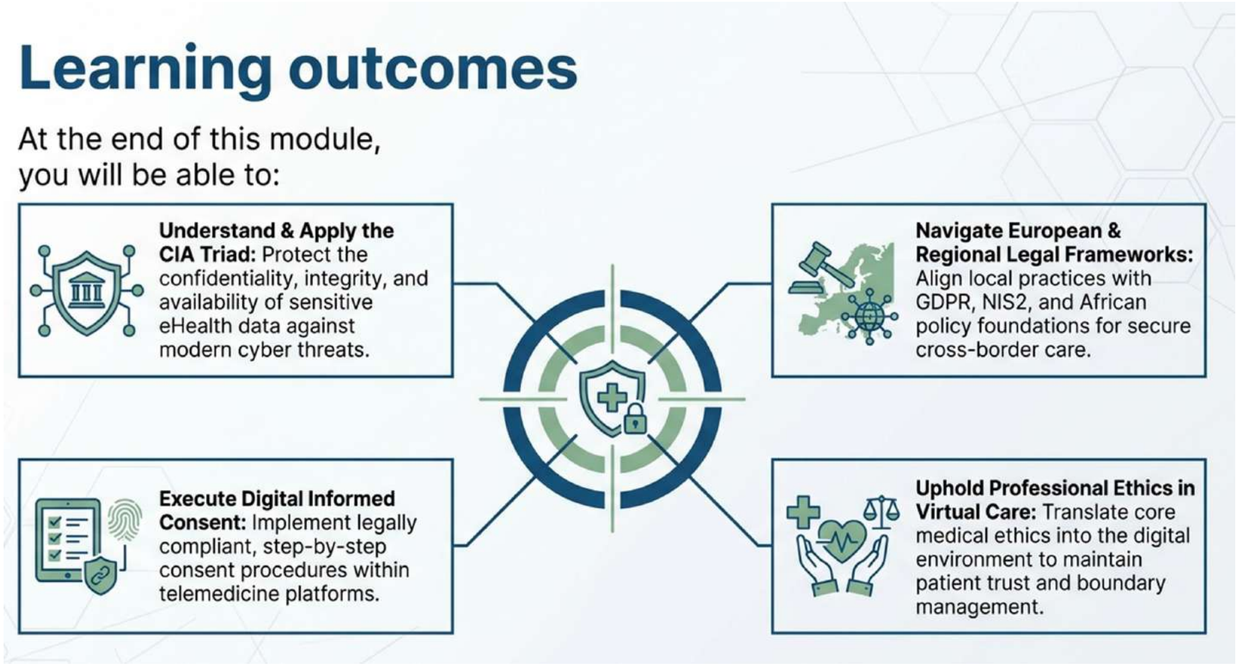
Capacity Building in the field of Higher Education

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Learning outcomes

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



- Explain the CIA triad (Confidentiality, Integrity, Availability) and apply it to eHealth scenarios.
- Identify common cybersecurity threats in healthcare and select appropriate technical and organisational mitigation strategies.
- Describe the European legal frameworks (GDPR, Patients' Rights Directive, NIS2, EU AI Act) and how they interact in digital health.
- Adapt NIS2 principles to African legal and policy contexts (Malabo Convention, regional frameworks).
- Design and implement valid informed consent procedures in telemedicine, including for cross-border and AI-assisted services.
- Apply core ethical principles and professional conduct standards in virtual consultations.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Index

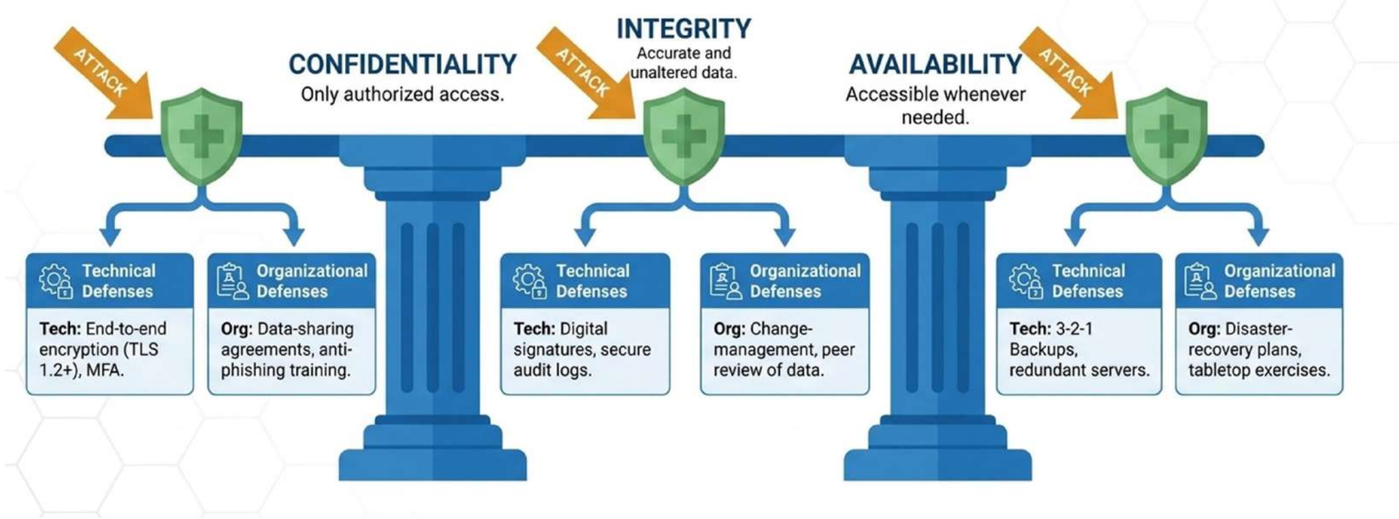
Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Unit 1 — Core Principles of Data Protection

• Confidentiality • Integrity • Availability

- Digital health (telemedicine, EHRs, AI diagnostics) transforms care but creates new risks for privacy, accuracy and availability of patient data.
- Every professional must understand the fundamental security principles before exploring threats or legal duties.
- This unit introduces the CIA triad — three pillars of data protection — and provides a common language for risk assessment, incident response, and compliance with GDPR and NIS2.
- Health data is among the most valuable personal information: targeted by criminals, strictly regulated, and critical for patient safety.
- A weakness in any one of the three pillars can compromise patient trust, disrupt care, and trigger heavy legal and financial penalties.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.2 The CIA Triad — Definitions

Three pillars of eHealth data protection

- **Confidentiality — Only authorised persons can access data.**
  - Example: A telemedicine platform allows only the attending physician and the patient to view video and test results.
- **Integrity — Data remain accurate, complete and unaltered from creation to use.**
  - Example: Electronic prescriptions are digitally signed so they cannot be modified without detection.
- **Availability — Data and services are accessible to authorised users whenever needed.**
  - Example: Remote-monitoring devices continuously upload readings to a cloud server clinicians can access 24/7.
- **Key Point: Protecting all three pillars simultaneously is critical. Strong encryption is useless if systems are unavailable in an emergency, and perfect uptime is meaningless if data can be secretly altered.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.3 Practical Controls

- **Technical and organisational measures for each pillar**

- **Confidentiality — Technical:**
  - End-to-end encryption, multi-factor authentication (MFA), role-based access control.
- **Confidentiality — Organisational:**
  - Data-sharing agreements, staff training on phishing and social engineering.
- **Integrity — Technical:**
  - Digital signatures, checksums, version control, secure audit logs.
- **Integrity — Organisational:**
  - Change-management procedures, peer review of data corrections.
- **Availability — Technical:**
  - Daily backups, redundant servers, disaster-recovery plans.
- **Availability — Organisational:**
  - Business-continuity planning, periodic recovery drills and tabletop exercises.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.4 Case A — Confidentiality Breach

- **Lost laptop with patient records**

- **Scenario:**
  - A clinical researcher copied patient datasets onto a personal laptop for home analysis. The laptop, containing unencrypted files, was stolen on a train.
- **CIA Impact: Confidentiality — health records of hundreds of patients exposed.**
- **Mitigation Plan:**
  - Enforce full-disk encryption on every portable device — even if hardware is lost, data remain unreadable without the key.
  - Activate remote-wipe technology so IT can erase data as soon as a device is reported missing.
  - Restrict export of patient data to personal equipment; require secure remote-access tools (VPN) instead of local copies.
  - Train staff regularly on safe handling of mobile devices, with annual simulated 'lost device' incidents.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.4 Case B — Integrity Failure

- **Altered clinical-trial data**

- **Scenario:**
  - An insider with administrator privileges manipulated lab results in an online clinical-trial database to improve perceived effectiveness of an experimental drug.
- **CIA Impact: Integrity — accuracy and reliability of clinical data compromised.**
- **Mitigation Plan:**
  - Apply principle of least privilege — grant only minimum rights per role.
  - Require MFA and heightened monitoring for all privileged accounts.
  - Maintain secure, tamper-evident audit logs of every data change; trigger automated alerts on unusual editing patterns.
  - Require dual approval / peer review for critical data changes.
  - Run periodic integrity audits with hash-based dataset verification.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.4 Case C — Availability Outage

- **Hospital ransomware attack**

- **Scenario:**
  - Ransomware encrypted core hospital servers, shutting down EHRs, lab systems and scheduling for 3 days. Staff reverted to paper, delaying surgeries and emergency care.
- **CIA Impact: Primarily Availability; confidentiality and integrity also at risk because attackers had full network access.**
- **Mitigation Plan:**
  - Robust patch-management programme to close known vulnerabilities.
  - Endpoint Detection and Response (EDR) tools that monitor and isolate infected machines automatically.
  - 3-2-1 backup strategy: 3 copies, 2 media, ≥1 offline; quarterly restoration tests.
  - Network segmentation so an infection in one department cannot spread.
  - Incident-response plan with 24/72-hour reporting timelines (GDPR/NIS2), rehearsed via tabletop exercises.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.4 Case D — Multi-Pillar Breach

- **Third-party cloud compromise**

- **Scenario:**
  - A cloud provider hosting a national telemedicine platform was hacked. Attackers accessed appointment schedules and disabled the service, leaving thousands of patients unable to reach doctors.
- **CIA Impact: All three pillars — confidentiality (leaks), integrity (risk of unauthorised modification), availability (downtime).**
- **Mitigation Plan:**
  - Strong vendor-risk management: ISO 27001 / SOC 2, annual security audits, fast breach notification clauses.
  - End-to-end encryption for all data exchanged with the cloud.
  - Continuous monitoring and anomaly detection on vendor interfaces.
  - Redundant hosting / fail-over so telemedicine can migrate to a secondary provider.
  - Joint incident-response exercises with vendors to clarify roles and reduce recovery time.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

1.5 Unit 1 — Key Points

Summary of Core Principles

- A single incident can compromise more than one CIA pillar; controls must address all three simultaneously.
- Effective protection requires both technical safeguards (encryption, backups, monitoring) and organisational measures (policies, contracts, staff training).
- A well-rehearsed incident-response plan dramatically reduces harm and regulatory penalties when a breach occurs.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Unit 2 — Cybersecurity Threats & Mitigation

- **Threats, case studies and layered defences**

Threat	CIA Impact	Layered Defenses
Phishing & Ransomware (e.g., WannaCry, HSE Ireland)	**Impact:** Availability & Confidentiality.	**Shield:** Patch management (<7 days), EDR offline backups, network segmentation.
Insider Threats (e.g., Vastaamo breach, altered trial data)	**Impact:** Integrity & Confidentiality.	**Shield:** Least-privilege access, multi-factor authentication, tamper-evident audit logs.
Supply-Chain / Cloud Compromise (e.g., SolarWinds)	**Impact:** Complete CIA Triad failure.	**Shield:** ISO 27001/SOC 2 vendor requirements, zero-trust architecture, continuous anomaly detection.

- **This unit covers four areas:**
  - Common cybersecurity threats in healthcare.
  - Real-world case studies showing impact.
  - Technical controls to reduce risk.
  - Organisational measures to sustain security.
- Healthcare faces the same threats as other sectors, but the stakes are higher because lives may be at risk.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.1 Common Cybersecurity Threats in eHealth

Most frequent attack types

- **Phishing & Social Engineering — fraudulent emails or calls trick users into revealing credentials or clicking malicious links.**
  - Impact: compromised EHR access, stolen credentials.
- **Ransomware — malicious software encrypts data and demands payment for decryption.**
  - Impact: hospital-wide downtime, cancelled appointments, potential patient harm.
- **Insider Threats — employees or contractors intentionally or accidentally compromise data.**
  - Impact: unauthorised data export, patient-record tampering.
- **Distributed Denial of Service (DDoS) — overwhelms servers with traffic to make services unavailable.**
  - Impact: telemedicine platform outages during critical consultations.
- **Supply-Chain Attacks — attackers compromise trusted vendors or software updates.**
  - Impact: malicious code injected into medical-device software or cloud services.
- **IoT / Medical Device Exploits — weakly secured connected devices become attack entry points.**
  - Impact: manipulated telemetry readings, unsafe device behaviour.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.2 The CIA Triad in Threat Context

Mapping threats to CIA pillars helps prioritise controls

- Phishing threatens Confidentiality by stealing credentials.
- Insider attacks often harm Integrity by altering records.
- Ransomware and DDoS primarily threaten Availability by disrupting services.
- Supply-chain attacks can compromise all three pillars at once via trusted channels.
- IoT exploits often harm Integrity (manipulated readings) and Availability (unsafe device behaviour).
- Mapping each threat to one or more CIA pillars allows organisations to design layered, prioritised controls.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.3 Case A — WannaCry & UK NHS (2017)

Global ransomware hits >80 NHS trusts

- **Scenario:**
  - WannaCry exploited an unpatched Windows vulnerability (MS17-010) and disrupted >80 NHS hospital trusts, cancelling ~19,500 appointments and diverting ambulances.
- **CIA Impact:**
  - Primary: Availability — critical systems inaccessible. Secondary: confidentiality risk from data exfiltration.
- **Root Causes:**
  - Delayed application of Microsoft's security patch and a flat network structure allowed the malware to spread rapidly.
- **Mitigation Plan:**
  - Robust patch management with critical updates applied within days.
  - Network segmentation to contain outbreaks; offline, tested backups.
  - Deploy EDR to isolate infected machines automatically.
- References: UK National Audit Office report on WannaCry; Microsoft security update MS17-010.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.3 Case B — Düsseldorf University Hospital (2020)

Ransomware contributes to patient death

- **Scenario:**
  - Ransomware disabled hospital IT, forcing emergency patients to be diverted. A critically ill patient died after a delayed transfer.
- **CIA Impact: Availability — emergency services interrupted.**
- **Root Causes:**
  - Exploited vulnerabilities in external-facing systems and inadequate emergency downtime procedures.
- **Mitigation Plan:**
  - Maintain downtime protocols (paper-based intake, alternative communications).
  - Conduct regular tabletop exercises.
  - Continuous vulnerability scanning with rapid patching.
- References: Europol press release; BSI Germany advisory 2020-1360.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.3 Case C — Vastaamo, Finland (2018-2020)

Mental-health records extorted

- **Scenario:**
  - Attackers accessed psychotherapy records and extorted both the clinic and individual patients, threatening to publish therapy notes.
- **CIA Impact: Confidentiality — highly sensitive mental-health data exposed.**
- **Root Causes:**
  - Inadequate database security and delayed breach detection.
- **Mitigation Plan:**
  - Encrypt sensitive records at rest; apply strict role-based access.
  - Continuous log monitoring with automated alerts for unusual database queries.
  - Establish a rapid breach-notification and victim-support process.
- References: Finnish Police press release; Data Protection Ombudsman case summary.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.3 Case D — Irish HSE (2021)

National-scale ransomware attack

- **Scenario:**
  - The Conti ransomware gang infiltrated Ireland's national health service, forcing a nationwide shutdown of hospital IT. Recovery cost hundreds of millions of euros.
- **CIA Impact: Availability — national-scale disruption; Confidentiality — data theft suspected.**
- **Root Causes:**
  - Prolonged attacker dwell time and insufficient network segmentation.
- **Mitigation Plan:**
  - Deploy a Security Operations Centre (SOC) with real-time threat detection.
  - Enforce MFA for all administrative accounts.
  - Use network segmentation to limit lateral movement.
- References: HSE Incident Report; Irish Government post-incident review.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.3 Case E — SolarWinds Supply-Chain (2020)

Trusted-update compromise affecting healthcare

- **Scenario:**
  - Attackers inserted malicious code into a widely used IT-management product. Many hospitals and research institutions were exposed.
- **CIA Impact: Confidentiality, Integrity, Availability — all potentially compromised.**
- **Root Causes:**
  - Over-reliance on trusted vendor updates and lack of verification mechanisms.
- **Mitigation Plan:**
  - Strengthen vendor risk management with third-party security certifications.
  - Signed-update verification and annual penetration tests.
  - Adopt zero-trust architecture to minimise damage even if a vendor is compromised.
- References: CISA advisory AA20-352A; SolarWinds security advisory.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.4 Technical Mitigation Strategies (1/2)

Layered defences — encryption, MFA, patching

- **Encryption**
  - Protect data at rest and in transit using strong, current algorithms (TLS 1.2+).
  - Encrypt backups and removable media.
- **Multi-Factor Authentication (MFA)**
  - Require at least two independent proofs of identity (password + authenticator app) for all privileged and remote accounts.
  - Stops most credential-theft attacks even if passwords are stolen.
- **Patch and Vulnerability Management**
  - Maintain an asset inventory and apply critical patches within 7 days of release.
  - Use automated vulnerability scanning to detect missing updates.
- **Network Segmentation**
  - Separate clinical from administrative networks; create secure 'jump boxes' for privileged access.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.4 Technical Mitigation Strategies (2/2)

Backups, monitoring, zero-trust, secure development

- **Secure Backups and Recovery**
  - Follow the 3-2-1 rule: 3 copies, 2 media, at least 1 offline.
  - Test restoration quarterly.
- **Logging and Monitoring**
  - Centralise logs and retain at least 90 days of records.
  - Automated alerts for unusual login patterns or data transfers.
- **Zero-Trust Architecture**
  - 'Never trust, always verify' — continuously authenticate users and devices.
- **Secure Development Practices**
  - For in-house software: code reviews, static analysis, and penetration tests before deployment.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.5 Organisational Mitigation Strategies (1/2)

Policy, risk, incident response, continuity

- **Information Security Policy**
  - High-level document approved by leadership; sets security objectives, responsibilities and reporting lines.
- **Risk Assessment & Treatment**
  - Annual risk assessments to identify critical assets, likely threats and mitigation priorities.
- **Incident Response Plan (IRP)**
  - Define roles, communication channels and actions for detection, containment, recovery and reporting.
  - Include 24/72-hour reporting procedures to comply with GDPR and NIS2.
- **Business Continuity & Disaster Recovery**
  - Plans to keep essential services running during outages.
  - Include paper-based fallbacks for patient registration and prescriptions.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

2.5 Organisational Mitigation Strategies (2/2)

- **Vendor security, DPIAs, training, accountability**

- **Vendor and Supply-Chain Security**
  - Include security clauses and breach-notification deadlines in all contracts.
  - Require vendors to demonstrate compliance with ISO 27001 or SOC 2.
- **Data Protection Impact Assessments (DPIAs)**
  - Mandatory under GDPR for high-risk processing such as telemedicine or AI diagnostics.
  - Identify potential risks before launching new services.
- **Training and Awareness**
  - Run regular phishing simulations; continuous education on safe data handling.
  - Reward staff for reporting suspicious incidents.
- **Management Accountability**
  - Boards and senior executives review cybersecurity KPIs quarterly and allocate adequate budgets.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Unit 3 — European Legal Frameworks for eHealth

GDPR, Patients' Rights, NIS2, EU AI Act

GDPR	Patients' Rights (2011/24/EU)	NIS2 Directive (2022/2555)	EU AI Act (2024)
Focus: Personal-data protection.	**Focus:** Cross-border patient care.	**Focus:** Cybersecurity of critical services.	**Focus:** Safety & transparency of AI.
Core Duty: Lawful processing & explicit consent.	**Core Duty:** Access to safe care, clear info & secure data exchange.	**Core Duty:** Risk management & 24/72-hour incident reporting.	**Core Duty:** High-risk management, human oversight, conformity testing.
Penalty: Up to€20M or 4% turnover.	**Penalty:** National penalties.	**Penalty:** Up to €10M or 2% turnover.	**Penalty:** Up to €35M or 7% turnover.

- Modern eHealth services depend on a complex mesh of EU laws.
- Four core frameworks must be considered together: GDPR (data protection), Patients' Rights Directive (cross-border care), NIS2 (cybersecurity of critical services), and the EU AI Act (safety and transparency of AI).
- DigHealth partners must integrate all four to ensure legal compliance, patient trust, and secure cross-border collaboration.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

3.1 GDPR — General Data Protection Regulation

Regulation (EU) 2016/679

- **Definition: The EU's primary law on personal-data protection. Applies to any organisation processing data of EU residents, even if based outside the EU.**
- **Key principles (Article 5):**
  - Lawfulness, Fairness, Transparency — valid legal basis, clearly explained.
  - Purpose Limitation — specific, explicit purposes.
  - Data Minimisation — only necessary data collected.
  - Accuracy — data kept up to date.
  - Storage Limitation — retain only as long as needed.
  - Integrity and Confidentiality — protect against unauthorised access or loss.
  - Accountability — controllers must demonstrate compliance.
- **Health data is special category data — requires explicit consent or another strong legal basis.**
- **Individual rights: access, correction, deletion, portability, objection.**
- **Penalties: up to €20 M or 4% of global annual turnover — whichever is higher.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

3.2 Patients' Rights Directive

Directive 2011/24/EU

- **Definition: Guarantees EU citizens can receive safe, high-quality healthcare across Member States and obtain reimbursement from their home country.**
- **Key Provisions:**
  - Patients may seek treatment abroad and claim reimbursement, subject to national rules.
  - Member States must provide clear information on providers, quality standards and reimbursement procedures.
  - Healthcare providers must ensure secure exchange of medical data for cross-border care.
- **Example:**
  - A Greek patient receiving telecardiology services from a German hospital must be informed about costs, service quality and data-exchange safeguards.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

3.3 NIS2 Directive

Directive (EU) 2022/2555 — minimum cybersecurity standards

- **Definition: Sets minimum cybersecurity standards and rapid incident-reporting obligations for critical sectors — healthcare, universities, digital infrastructure.**
- **Scope: Essential entities (hospitals, major telemedicine platforms) and Important entities (university research centres).**
- **Core Obligations:**
  - Risk Management — encryption, access control, supply-chain security, incident response.
  - Incident Reporting — early warning ≤24 h, detailed report ≤72 h, final report ≤1 month.
  - Management Accountability — senior leadership approves security policies and can be personally liable.
- **Penalties: up to €10 M or 2% of global turnover for essential entities.**
- **Example: A university hospital in a DigHealth pilot must show network segmentation, MFA and a 24/72-hour reporting process to comply with NIS2.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

3.4 EU AI Act (2024)

Risk-based regulation of AI systems

- **Definition: World's first comprehensive AI law — risk-based approach to regulate AI systems that could harm health, safety or fundamental rights.**
- **Risk Categories:**
  - Unacceptable Risk — prohibited uses (e.g., social scoring).
  - High Risk — AI used in medical diagnosis, triage or treatment recommendations.
  - Limited / Minimal Risk — subject only to transparency rules.
- **Obligations for High-Risk AI:**
  - Risk-management systems and high-quality, representative datasets.
  - Human oversight and transparency — users know they are interacting with AI.
  - Pass a conformity assessment before deployment in the EU.
- **Example: An AI tool recommending cancer treatment must document training data, allow human override, and undergo formal EU conformity testing.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

3.5 How the Frameworks Interact

One eHealth project may need to comply with all four

- **GDPR — focus on personal-data protection; max fine €20 M or 4% turnover.**
- **Patients' Rights Directive — cross-border patient care; national penalties.**
- **NIS2 — cybersecurity of critical services; max fine €10 M or 2% turnover.**
- **EU AI Act — safety and transparency of AI; max fine €35 M or 7% turnover (severe breaches).**
- **Example: an AI-based telemedicine service must:**
  - Obtain GDPR-compliant consent for patient data.
  - Provide cross-border access and reimbursement under the Patients' Rights Directive.
  - Implement NIS2 cybersecurity measures and 24/72-hour incident reporting.
  - Pass a high-risk AI conformity assessment under the AI Act.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Unit 3 — Key Points

- **Integrated EU compliance for eHealth**

GDPR protects personal and health data and grants patients strong control over their information.	The Patients' Rights Directive ensures safe, reimbursable cross-border healthcare.	NIS2 sets minimum cybersecurity standards and strict incident-reporting timelines.	The EU AI Act regulates AI by risk level, imposing strict controls on high-risk medical applications.	DigHealth partners must integrate all four frameworks for legal compliance, patient trust and secure cross-border collaboration.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Applying NIS2 Principles in African Countries

Introduction

- NIS2 (Directive (EU) 2022/2555) sets common cybersecurity standards and fast incident-reporting requirements for critical sectors in the EU — healthcare, higher education and digital infrastructure.
- Although legally binding only in the EU, its principles can guide African governments, universities and health authorities that want to:
  - Strengthen cybersecurity.
  - Align with international best practice.
  - Facilitate secure cross-border cooperation with European partners.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 1. Core Ideas of NIS2

Technology-neutral concepts adaptable to African contexts

- **Risk-management measures: encryption, MFA, network segmentation, supply-chain security.**
- **Incident reporting: early warning ≤24 h; detailed report ≤72 h; final report ≤1 month.**
- **Management accountability: senior leadership approves cybersecurity policies and can face penalties.**
- EU Official text: Directive (EU) 2022/2555 (EUR-Lex).
- These concepts — sector classification, minimum controls, rapid reporting, top-level accountability — are technology-neutral and can be adapted to African contexts.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 2. Legal & Policy Foundations

Existing African frameworks as legal gateways

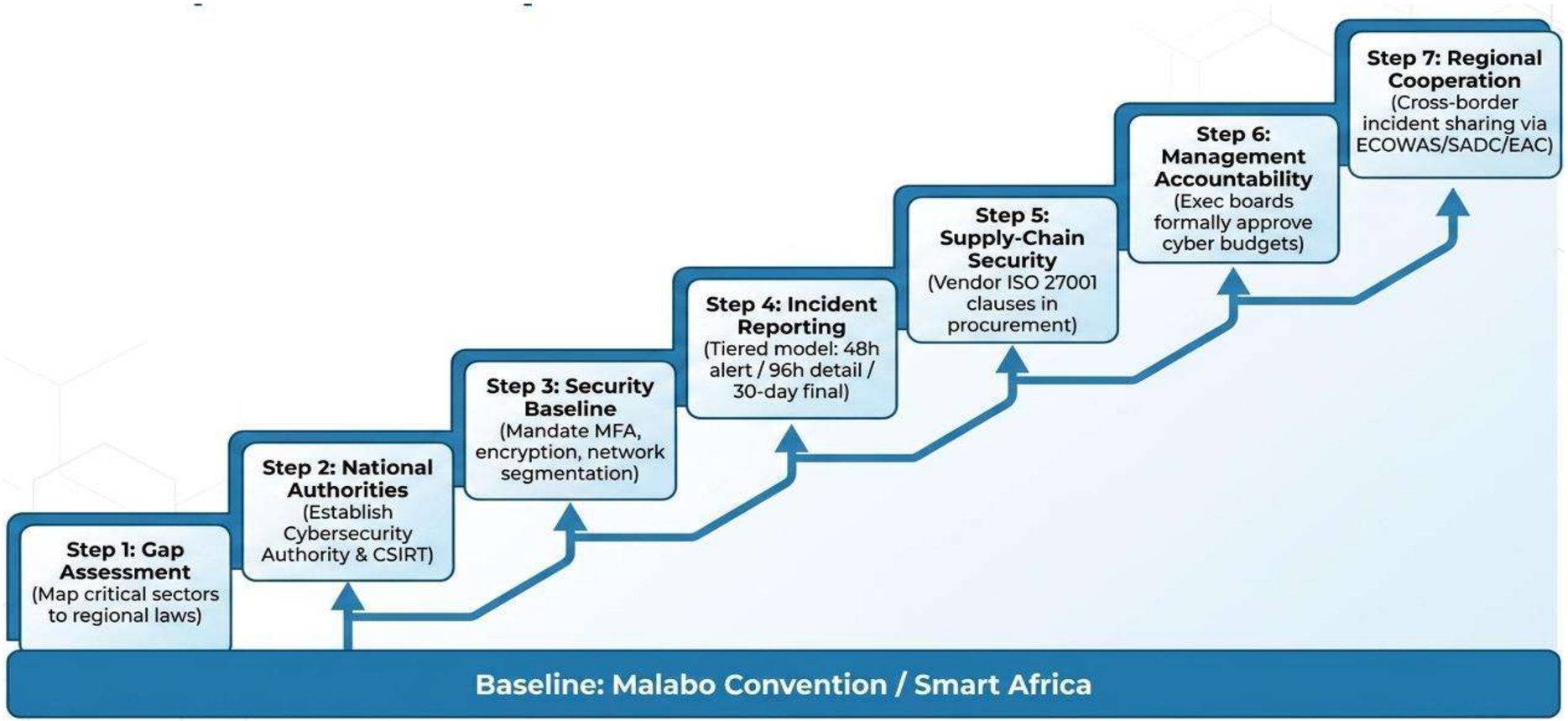
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) — continental treaty in force June 2023.
- AU Digital Transformation Strategy for Africa 2020-2030 — secure digital infrastructure and harmonised cyber policies.
- Smart Africa Cybersecurity Blueprint — continental blueprint for CSIRTs and regional cooperation.
- ECOWAS Directive on Fighting Cybercrime (2011) and Supplementary Act on Personal Data Protection (2010).
- SADC Model Laws on Data Protection & Cybercrime (2012) — templates for Southern African states.
- EAC Cybersecurity Framework — guidelines for harmonised cyber legislation in East Africa.

These instruments provide a legal backbone for NIS2-style obligations.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 3. Step-by-Step Adaptation



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 3. Step-by-Step Adaptation (1/2)

Phases 1-3

Phase 1 — Gap Assessment

- Map existing national laws against the Malabo Convention and regional model laws.
- Identify critical sectors (health, energy, transport, education) and key operators (hospitals, telecoms, research universities).

Phase 2 — Establish National Authorities

- Designate or strengthen a National Cybersecurity Authority and a CSIRT to receive incident reports.
- Examples: Kenya's KE-CSIRT or South Africa's CSIRT as focal points.

Phase 3 — Minimum Security Baseline

- Publish national guidelines requiring core controls (MFA, encryption of health data, patch management, network segmentation).
- Align with NIS2 Annex I & II risk-management measures for critical and important entities.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 3. Step-by-Step Adaptation (2/2)

Phases 4-7

Phase 4 — Incident Reporting Scheme

- Tiered reporting (e.g., 48 h early alert, 96 h detailed, 30 d final), mirroring NIS2 24/72-hour standard.
- Secure national portal for reporting and threat-intelligence sharing.

Phase 5 — Supply-Chain Security

- Government contracts and healthcare procurement: vendor security clauses, ISO 27001 / SOC 2, breach-notification duties.

Phase 6 — Management Accountability

- Boards and senior executives of hospitals, universities and critical providers approve cybersecurity budgets and risk reports.

Phase 7 — Regional Cooperation

- Connect national CSIRTs to Smart Africa or regional networks (ECOWAS, SADC, EAC) for cross-border incident sharing and joint exercises.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 Toolkit — A. Minimum Security Baseline (1/2)

Identity, data, vulnerability, backups

- **A1. Identity & Access Management**
  - MFA everywhere for privileged, remote, email and VPN accounts.
  - Least-privilege roles; quarterly access reviews; immediate de-provisioning on exit.
  - Dedicated break-glass accounts stored offline and audited.
- **A2. Data Protection**
  - TLS 1.2+ on all web services; HSTS enabled.
  - Encrypt data at rest for databases, object storage, backups, laptops.
  - Pseudonymise for research / secondary use; document key management.
- **A3. Vulnerability & Patch Management**
  - Complete asset inventory (servers, apps, endpoints, IoT/medical devices).
  - Critical patches within 7 days, high severity within 14 days; quarterly authenticated scans.
- **A4. Backups & Recovery**
  - 3-2-1 rule (3 copies, 2 media, 1 offline/immutable); quarterly restore drills with measured RTO/RPO.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 Toolkit — A. Minimum Security Baseline (2/2)

Network, monitoring, IR, supply chain

- **A5. Network Security**
  - Segment clinical/OT, corporate IT and guest environments.
  - Jump-hosts for admin access; disable direct admin logins.
  - EDR on servers and workstations with integrated alerting.
- **A6. Logging & Monitoring**
  - Centralised logs (auth, firewall, EDR, application) ≥90 days online / 1 year archive.
  - Alerts on failed MFA bursts, new admin creation, large data extractions, malware quarantines.
- **A7. Incident Response (IR)**
  - At least three one-page playbooks: phishing, ransomware, data leak.
  - 24/7 contacts list; communications templates; tabletop exercises every 6 months.
- **A8. Supply-Chain Security**
  - Procurement: MFA for vendor admins, encryption, breach-notification SLA, annual independent security test letter.
  - Cloud: region/location pinning and, where possible, customer-managed keys.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 Toolkit — B. Incident Reporting Scheme

Adoptable timers and minimum fields

Who reports?

- Essential Entities: national hospitals, national eHealth platforms, national research networks.
- Important Entities: universities handling health data, regional hospitals, major ISPs supporting health.

When?

- Early Alert: ≤48 h of awareness (target 24 h as maturity grows).
- Detailed Notification: ≤96 h with initial root cause and impact.
- Final Report: ≤30 days with corrective actions and lessons learned.

Minimum fields:

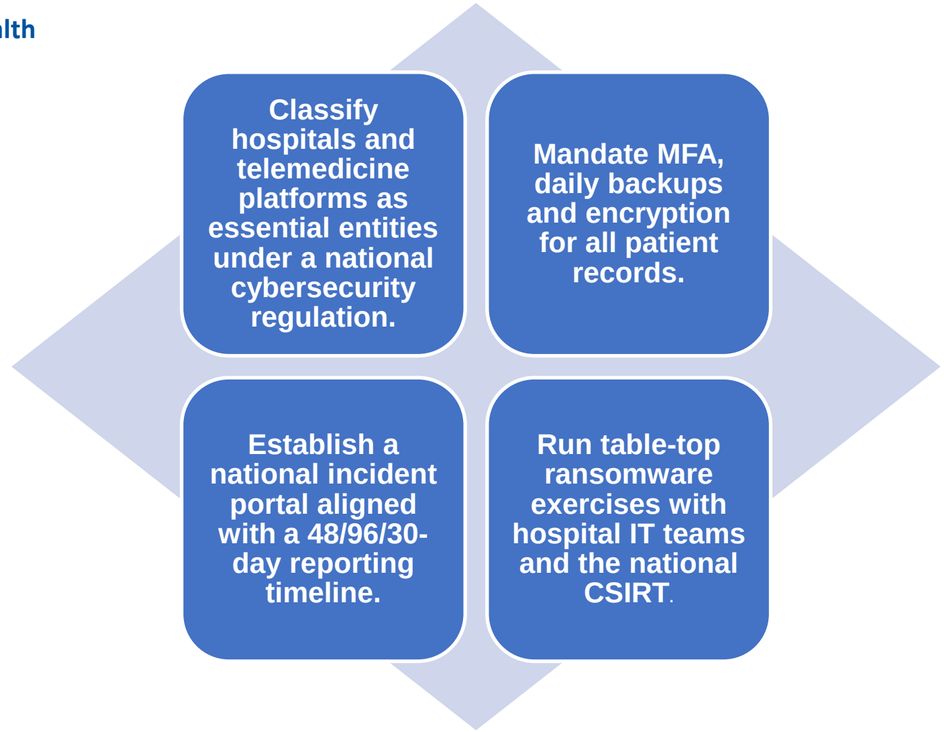
- Entity, contacts, affected services/systems, CIA impact, number of patients/data records affected, event timeline, immediate containment, assistance requested, preliminary root cause, cross-border implications.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 4. Health Sector Pilot

- **Practical example for a Ministry of Health**



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

NIS2 in Africa — 5. Benefits of Adoption

Why it matters for African health systems

- ✓ Improved resilience of health systems against ransomware and data breaches.
- ✓ Stronger international cooperation — easier participation in EU-funded research and Erasmus+ projects.
- ✓ Legal harmonisation with global partners, facilitating cross-border data exchange and telemedicine.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Unit 4 — Informed Consent in Telemedicine

Introduction

- Informed consent is a cornerstone of ethical healthcare and a key legal requirement under GDPR, the Patients' Rights Directive and international medical ethics codes.
- Telemedicine — where consultations, diagnosis and treatment occur remotely — presents new challenges:
  - Patients may never meet their provider in person.
  - Digital platforms can obscure how and where data are stored.
  - Cross-border services create overlapping legal obligations.

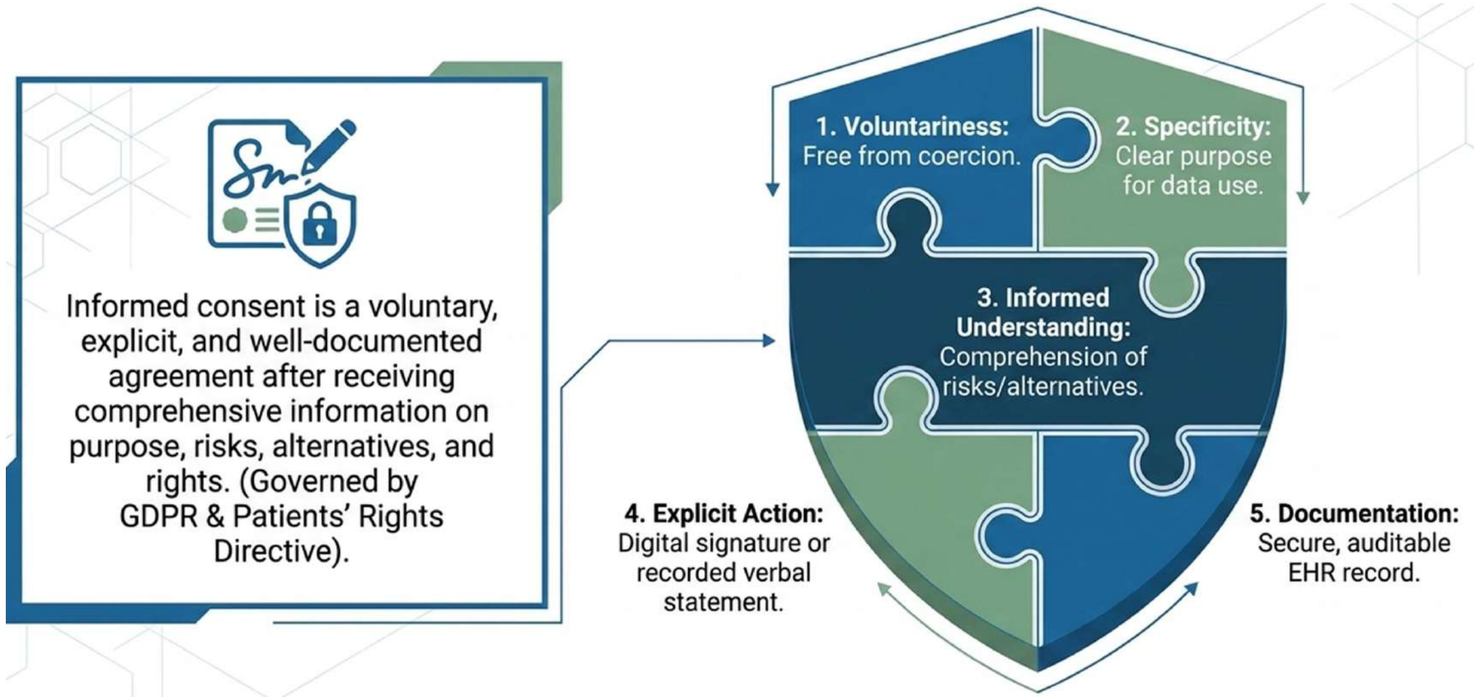
This unit explains how to obtain and document valid informed consent in digital health environments.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.1 Definition of Informed Consent

Five required elements



Informed consent is a voluntary, explicit, well-documented agreement by a patient to allow a provider or researcher to perform a service or process personal data after receiving comprehensive information on purpose, risks, benefits, alternatives and rights of withdrawal.

- **Voluntariness — the decision is free from coercion or undue influence.**
- **Specificity — the consent clearly states each purpose for which data will be used.**
- **Informed understanding — the patient comprehends procedure, risks and alternatives.**
- **Explicit action — a clear affirmative step (digital signature, recorded verbal statement).**
- **Documentation — a secure, auditable record of the consent and any subsequent withdrawal.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.2 Legal Foundations

Key instruments for telemedicine consent

GDPR — requires explicit consent for processing health data and mandates clear withdrawal mechanisms.

Reference: eur-lex.europa.eu/eli/reg/2016/679/oj.

Patients' Rights Directive (2011/24/EU) — guarantees access to clear information and informed decision-making in cross-border healthcare.

Reference: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0024.

World Medical Association — Declaration of Helsinki — international ethical standards for medical research and clinical care.

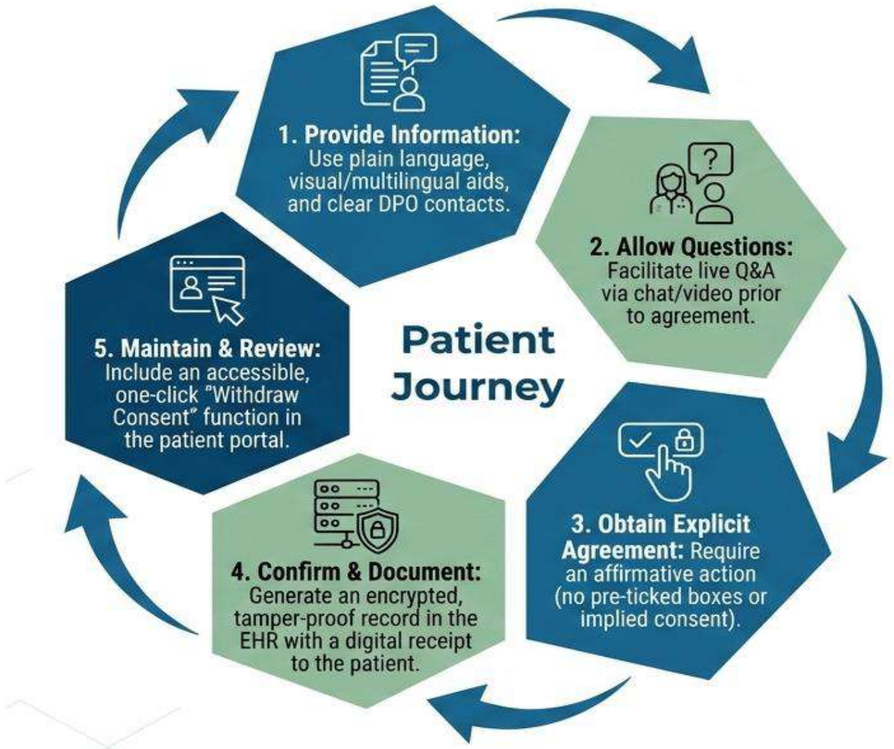
Reference: wma.net/policies-post/wma-declaration-of-helsinki-…

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.3 Step-by-Step Digital Consent Process

Five steps from information to withdrawal



- **1. Provide Information — clear explanation of the service, purpose of data collection, risks, benefits, retention, DPO contact.**
  - Plain language and visual aids; multilingual versions; audio/video formats for low literacy.
- **2. Allow Questions — give the patient time to ask questions via chat, phone or video before consent.**
  - Keep a record of Q&A to improve future materials.
- **3. Obtain Explicit Agreement — affirmative action: ticking a checkbox, signing digitally, recorded verbal consent.**
  - No pre-ticked boxes or implied consent.
- **4. Confirm and Document — provide a digital receipt or PDF; store a tamper-proof record in the EHR.**
  - Use audit trails and encryption.
- **5. Maintain & Review — allow withdrawal at any time; log all withdrawals.**
  - Include a one-click 'Withdraw Consent' function on patient portals.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.4 Digital Tools for Consent

Practical instruments for telemedicine

- Secure e-signature platforms (e.g., DocuSign, Adobe Sign) compliant with eIDAS and GDPR.
- Integrated EHR consent modules that automatically log timestamps and user IDs.
- Video consent recording for patients with low literacy, stored on encrypted servers.
- Multilingual mobile apps allowing patients to read or listen to consent information in their preferred language.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.5 Case 1 — Tele-Psychiatry Service

Recordings without clear retention or purpose

- **Scenario:**
  - A provider records therapy sessions for 'research purposes' but fails to specify retention periods, security measures or secondary uses.
- **Risks:**
  - Patients cannot make a fully informed decision (GDPR Articles 6 & 9).
  - Unclear retention and purpose create risk of unlawful processing and reputational damage.
- **Mitigation:**
  - Rewrite consent notice — list each purpose, storage duration, DPO contact; provide plain-language and multilingual versions.
  - Re-collect consent via secure email / patient portal, with explicit affirmative action.
  - Encrypt all recordings at rest and in transit (AES-256/TLS 1.2+); store keys separately.
  - Build a 'withdraw consent' button that triggers removal from active research sets, deletion/anonymisation, confirmation email and audit log.
  - Quarterly retention-log audits to verify deletion / anonymisation rules are applied.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.5 Case 2 — Cross-Border Cardiology

Tele-consultation across jurisdictions

- **Scenario:**
  - An Ethiopian patient receives a tele-consultation from an EU cardiology clinic. Different jurisdictions and unclear data-transfer safeguards create legal uncertainty.
- **Risks:**
  - GDPR applies to the EU clinic; local privacy laws may impose additional duties.
  - Cross-border transfer without safeguards may violate GDPR Chapter V.
- **Mitigation:**
  - Map data flows; identify safeguards (Standard Contractual Clauses, Binding Corporate Rules, or explicit consent for transfer).
  - Cross-border consent: patient is informed that data is transferred to/from the EU, the legal basis, and rights under both GDPR and local law.
  - Provide a dedicated EU-based DPO contact; create a dual-channel withdrawal process (EU provider or local partner).
  - Review the arrangement annually; document all transfers in the clinic's Article 30 Records of Processing.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.5 Case 3 — AI Diagnosis

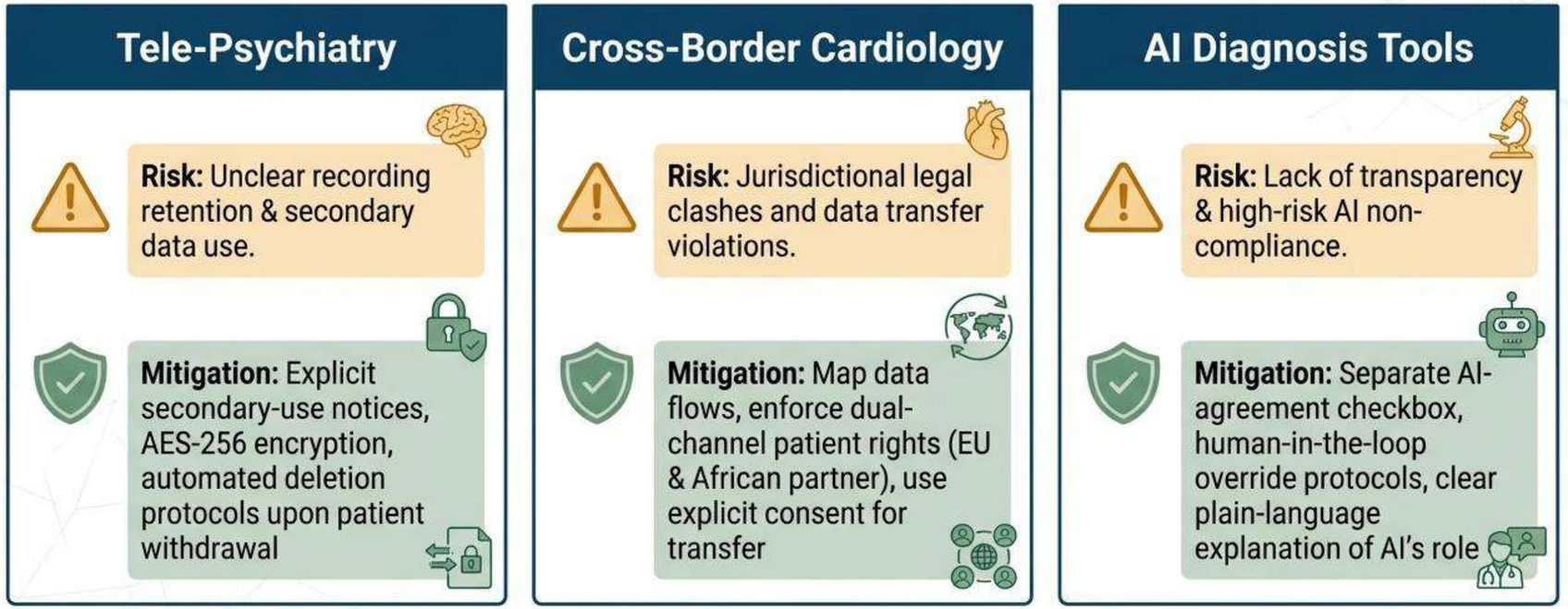
Triage AI without transparency to patients

- **Scenario:**
  - An AI triage tool generates treatment suggestions, but the provider does not explain the AI's role to the patient.
- **Risks:**
  - Lack of transparency breaches GDPR Articles 13–15 and EU AI Act high-risk obligations.
  - Patients may misunderstand the human oversight in decision-making.
- **Mitigation:**
  - Transparency statement — what the AI does, its limitations, that a clinician reviews all AI outputs.
  - Consent form: separate checkbox confirming the patient understands and agrees to AI involvement; link to detailed explanation.
  - Human-oversight protocol: clinicians validate every AI recommendation; log overrides and justifications.
  - Risk assessment under EU AI Act high-risk requirements; document training data, accuracy metrics and bias testing.
  - Offer patients the option to receive care without AI support — opting out must not delay or diminish service.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Cases — Diagnosis



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.6 Ethical Considerations

Beyond legal compliance

- **Respect for Autonomy: consent is an ongoing dialogue, not a one-time signature.**
- **Equity :accessible materials for persons with disabilities and diverse languages.**
- **Transparency :disclose use of third-party platforms or AI algorithms.**
- **Data Minimisation : collect only data strictly necessary for the consultation.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

4.7 Checklist for Telemedicine Providers

Confirm before every virtual consultation

- ❑ Patient identity and location are verified.
- ❑ Platform is encrypted and compliant with GDPR security standards.
- ❑ Consent has been obtained and is documented in the EHR.
- ❑ Patient is informed about data processing, retention and DPO contact.
- ❑ Withdrawal mechanism is available and clearly explained.
- ❑ For cross-border care: legal basis for transfer, applicable safeguards and dual-channel contact are in place.
- ❑ For AI-assisted care: transparency statement, human oversight and opt-out option are provided.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Ethics in Virtual Consultations — Introduction

From in-person to digital ethics

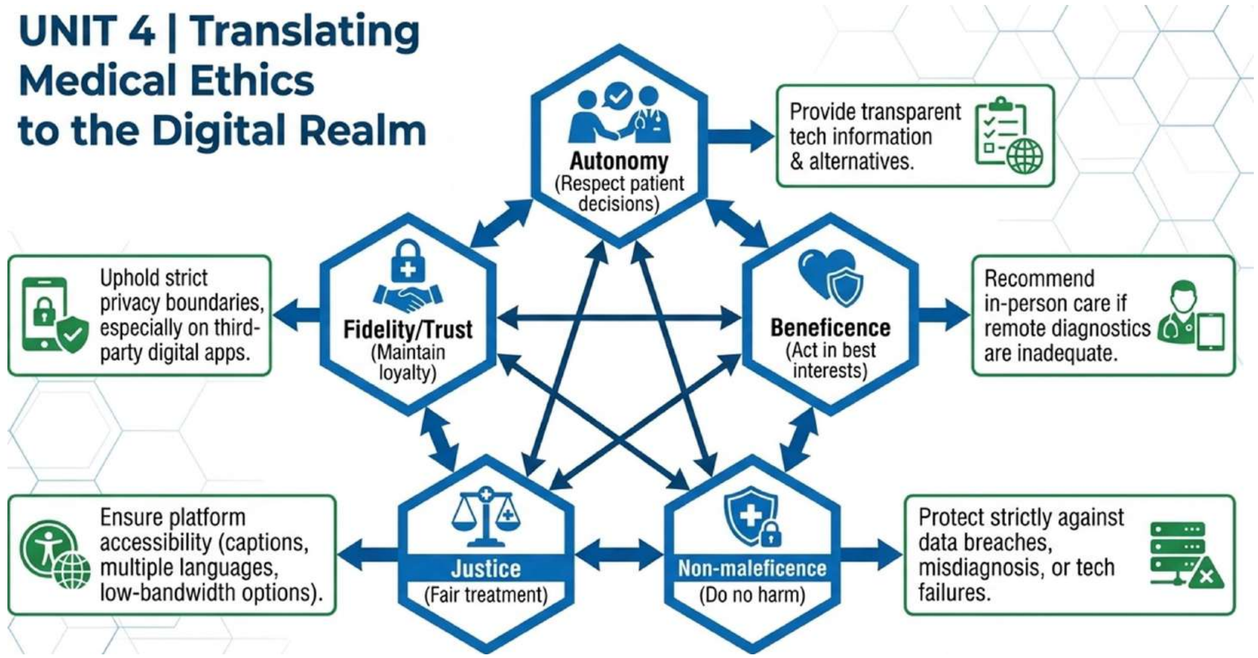
- Virtual consultations — telemedicine platforms, mobile apps, video calls — are now a core part of healthcare delivery.
- Benefits: accessibility, continuity of care, cost savings.
- New ethical challenges:
  - Maintaining professional boundaries when consulting from a patient's living room.
  - Preserving confidentiality when platforms transmit sensitive health data.
  - Building trust when human cues are limited to a screen.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

5.1 Core Ethical Principles

Digital interpretation



- **Autonomy — respect the patient's right to make informed decisions.**
  - Provide complete, understandable information about the telemedicine process, technology and limitations.
- **Beneficence — act in the patient's best interest.**
  - Ensure the chosen modality is clinically appropriate; recommend in-person care if remote care is inadequate.
- **Non-maleficence — do no harm.**
  - Protect against data breaches, misdiagnosis from poor video quality, or delays from technical failures.
- **Justice — fair and equal treatment.**
  - Provide accessible platforms (multilingual, captions, disability accommodations) and equitable scheduling.
- **Fidelity / Trust — uphold privacy and security promises, even when using third-party platforms.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

5.2 Professional Conduct (1/2)

Challenge vs. Standard	Action Checklist
Environment & Prep:	**USE** a private, well-lit space. **TEST** equipment and network connections beforehand. 
Patient Verification:	**VERIFY** identity (using 2 identifiers) and physical location to enable emergency routing. 
Communication:	**OBTAIN** verbal consent confirmation at the start. **AVOID** technical jargon; maintain eye contact via the camera. 
Confidentiality:	**USE** only encrypted, GDPR-compliant platforms. **NEVER** store session data or video on personal devices. 
Boundaries:	**DOCUMENT** all communication in the official EHR. **AVOID** informal messaging or social media contact with patients. 

- **1. Preparation and Environment**
  - Private, quiet, well-lit space free from interruptions.
  - Test camera, microphone and network before the consultation.
  - Patient records and diagnostic tools accessible.
- **2. Patient Verification**
  - Confirm identity using at least two identifiers (name and date of birth).
  - Verify location for jurisdictional compliance and emergency response capability.
- **3. Communication Etiquette**
  - Explain the structure of the visit; obtain verbal confirmation of consent.
  - Speak clearly, maintain eye contact through the camera, use plain language.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

5.2 Professional Conduct (2/2)

Challenge vs. Standard	Action Checklist
Environment & Prep:	**USE** a private, well-lit space. **TEST** equipment and network connections beforehand.
Patient Verification:	**VERIFY** identity (using 2 identifiers) and physical location to enable emergency routing.
Communication:	**OBTAIN** verbal consent confirmation at the start. **AVOID** technical jargon; maintain eye contact via the camera.
Confidentiality:	**USE** only encrypted, GDPR-compliant platforms. **NEVER** store session data or video on personal devices.
Boundaries:	**DOCUMENT** all communication in the official EHR. **AVOID** informal messaging or social media contact with patients.

- **4. Confidentiality and Data Handling**
  - Remind patients to join from a private location and use a secure device.
  - Use only encrypted, GDPR-compliant platforms; never store recordings on personal devices.
- **5. Boundary Management**
  - Maintain the same professional boundaries as in-person visits — no informal messaging on personal accounts, no social-media contact.
  - Document all communications in the official EHR.
- **6. Emergency Protocols**
  - Clear plan for urgent situations (sudden deterioration).
  - Directory of local emergency numbers and patient location at the start of the session.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

5.3 Practical Challenges and Mitigation

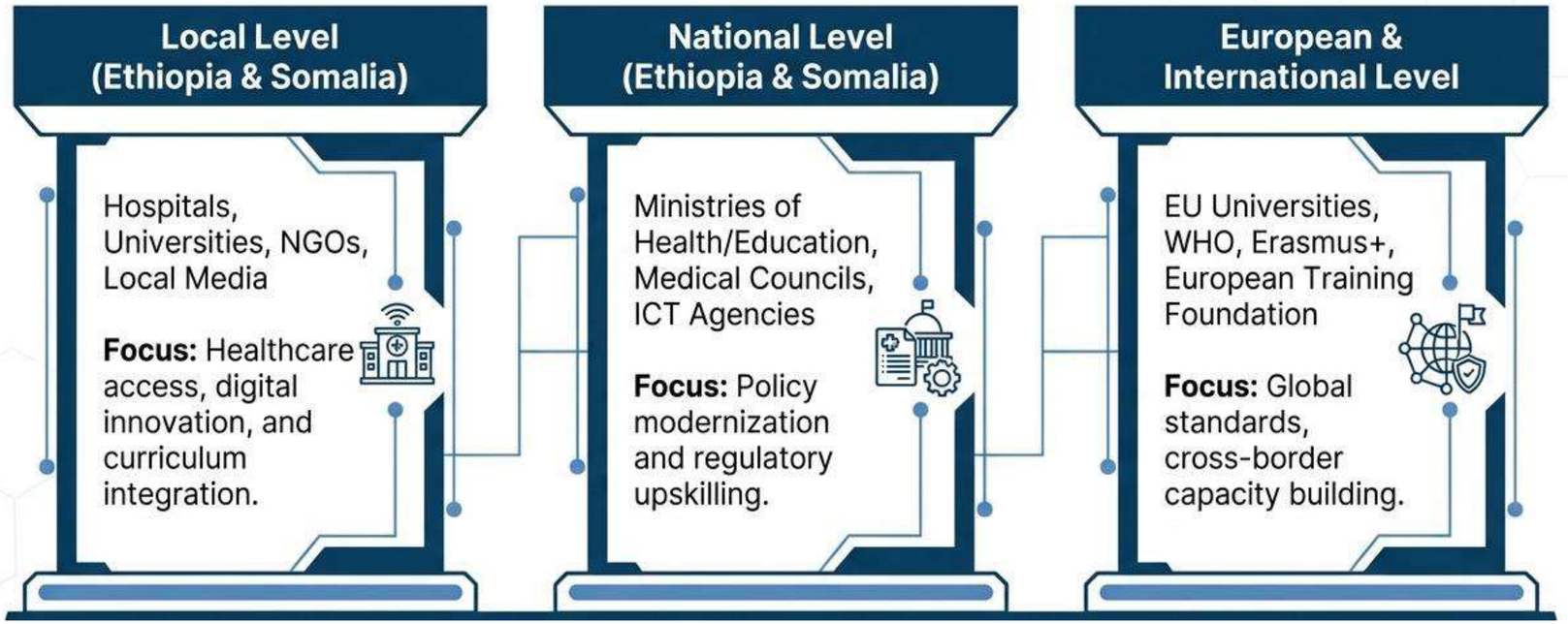
Bridging technology, equity and law

Technical failures — risk of interrupted care or miscommunication.	Data breaches — exposure of sensitive health data.	Digital divide — exclusion of patients with limited internet or devices.	Cross-border jurisdiction — conflicting legal requirements.
• Mitigation: fallback options (telephone, reschedule), test equipment beforehand.	• Mitigation: end-to-end encrypted platforms, MFA, strict access controls.	• Mitigation: hybrid options (community tele-kiosks, telephone consultations), clear guidance and tech support.	• Mitigation: verify patient location, inform about applicable laws, obtain consent for cross-border transfers.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Target Groups for DigHealth Dissemination



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Summing up

1. **CIA Triad** — Confidentiality, Integrity and Availability are the three pillars of eHealth data protection — controls must address all three simultaneously.
2. **Threats & Mitigation** — Phishing, ransomware, insider threats, DDoS, supply-chain and IoT attacks need layered technical and organisational defences.
3. **EU Legal Frameworks** — GDPR, the Patients' Rights Directive, NIS2 and the EU AI Act interact — eHealth services must integrate all four for compliance.
4. **Consent & Ethics** — Valid informed consent, transparency for AI, cross-border safeguards and ethical conduct are essential in virtual care.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

In Summary the Action Plan

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Thank you!

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.