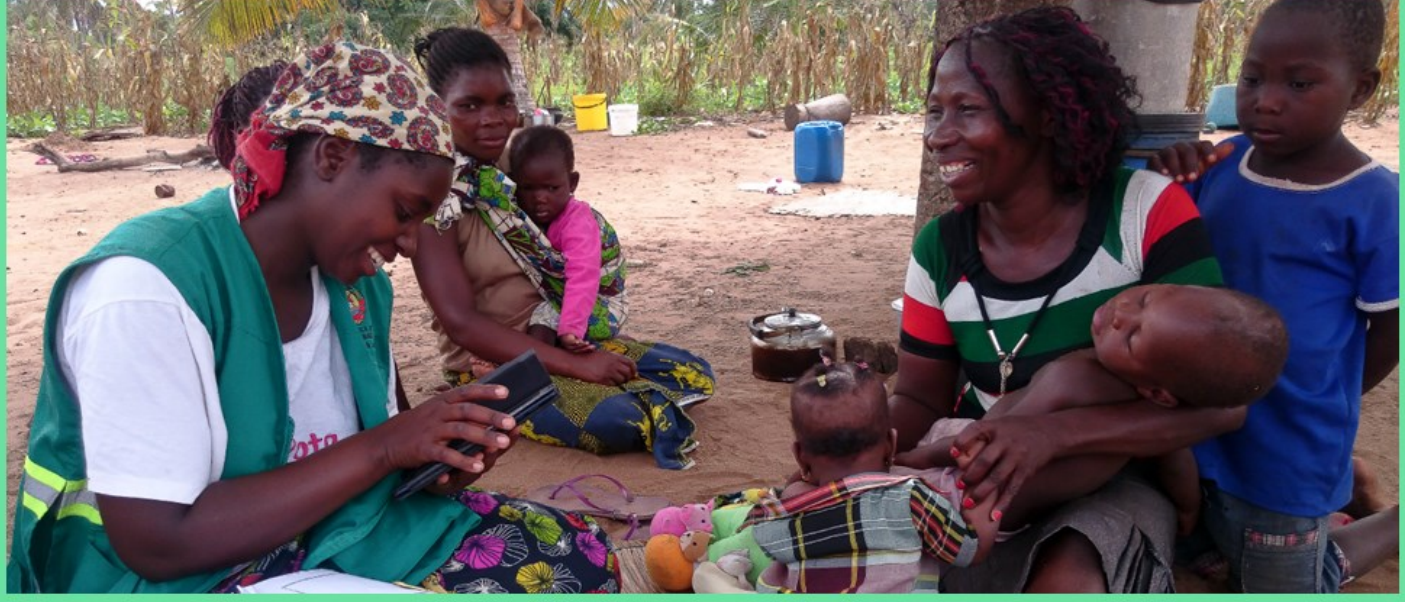

Stepwise toolkit on cybersecurity, confidentiality, and privacy for planning and operationalizing patient-centric digital health systems

DICE | Digital Health Centre of Excellence

The DICE consortium

Contents

List of abbreviations

ABAC	Attribute-Based Access Control
ABDM	Ayushman Bharat Digital Mission
ACL	Access Control List
CERT	Computer Emergency Response Team
DHIs	Digital Health Interventions
DLP	Data Loss Prevention
EHR	Electronic Health Records
ESPs	Essential Service Providers
EU	European Union
GDHCN	Global Digital Health Certification Network
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIV	Human Immunodeficiency Virus
ICT	Information and Communications Technology
ISCM	Information Security Continuous Monitoring
IoT	Internet Of Things
LGBTQIA+	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, Asexual, Plus all other identities
LMICs	Low- and Middle-Income Countries
MoH	Ministry of Health
NCA	National Cybersecurity Agency
NIST	National Institute of Standards and Technology
OTP	One Time Passwords
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SIEM	Security Information and Event Management
SSL	Secure Socket Layer
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
WHO	World Health Organization

Glossary

Term	Definition
Availability	Ensuring timely and reliable access to and use of information.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Cybersecurity	The practice of protecting data, computer systems and networks from digital attacks such as unauthorized access, tampering and shutdown.
Cybersecurity maturity level	The extent to which a country has optimized cybersecurity systems and processes.
Control objectives	Statements of the desired states you want to achieve through your security measures that act as guiding principles for choosing and implementing controls, ensuring your efforts target specific vulnerabilities and protect your assets effectively.
Cybersecurity event	A positive or negative change in cybersecurity systems that may have an impact on an organization's operations.
Cybersecurity incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity and availability of information or an information system that warrants response to the incident.
Cybersecurity program	Set of procedures, policies, guidelines, and standards that a country puts in place to monitor, detect, and respond to cyber threats.
Data privacy	Assurance of the proper handling and confidentiality of personal data.
Integrity	The protection of data and systems from unauthorized, intentional, or accidental, unauthorized alteration.
Managed services	Outsourced IT solutions provided by a third-party. In this model, the external provider takes responsibility for planning, implementing, maintaining, and supporting IT functions and systems on behalf of their clients.
Open access	Free access to scholarly literature over the internet that is accessible and reusable for everyone.
Risk management	The program and supporting processes to manage security risks to organizational operations, assets, individuals, and other organizations, and encompasses context establishment for risk-related activities, risk assessment, risk response and risk monitoring over time

Risk owner	The person or entity responsible for managing and mitigating a specific risk. They ensure understanding, implement controls, and monitor the risk over time.
Risk treatment	The process of selecting and implementing controls to modify the likelihood and impact of identified cyber threats. It is the action phase of risk management, where you move from passive awareness to proactive mitigation.
Trust network	A secure, technical environment that facilitates exchange of sensitive data among participants in the network.

1. Introduction

The increased use of digital technologies in healthcare necessitates an increased commitment to ensuring continued access to timely and critical health services with client privacy and confidentiality through secure and resilient digital systems. Securing digital health systems prevents unauthorized access to sensitive health information, preserving patient privacy and confidentiality. The WHO Global strategy on digital health 2020-2025 (1) classifies health data as sensitive personal data requiring extra security measures. It also emphasizes the need for robust legal and regulatory frameworks to protect the privacy, confidentiality, and integrity of health data.

Aligned with the WHO Global strategy on digital health 2020-2025, this toolkit aims to create cybersecurity awareness and offer guidance on planning and budgeting for cybersecurity and privacy protection of digital health interventions (DHIs), including patient-centric and individual-level digital systems. This document is for a non-technical audience who are pivotal in shaping and implementing patient-centered health systems at various levels. The toolkit is designed to facilitate the implementation of secure and privacy protecting DHIs by articulating a stepwise approach to integrating cybersecurity measures across the DHI lifecycle.

Cybersecurity refers to processes and methodologies employed to safeguard computers, servers, mobile devices, networks, and data against unauthorized access and breaches. The national Institute of Standards and Technology Cyber Security Framework, (NIST CSF) (2) within the health context, cybersecurity describes the tools, policies, guidelines, risk management approaches, best practices and technologies that can be used to protect the availability, safety, effectiveness, integrity and confidentiality of health data, critical infrastructure, medical devices and other DHIs. Healthcare Information and Management Systems Society (HIMSS, 2023)(2).

Data protection is the safeguarding of crucial data from corruption, compromise, or loss, with the ability to restore it to a functional state if inaccessible. It ensures data integrity, authorized access, and compliance with legal requirements, making data available and usable as intended (3).

Privacy protection in healthcare, centers on safeguarding individuals' personal health information through stringent measures to prevent unauthorized access, use, or disclosure of protected health information (PHI), ensuring confidentiality and upholding privacy rights (3).

2. Building the case for secure digital health systems

Digital health systems are particularly vulnerable to cyber-attacks due to several factors:

- The intrinsic value of health data, characterized by its sensitive nature and significant market worth, makes it an attractive target for cyber-attacks (4);
- Reliance on outdated legacy digital health systems renders them vulnerable to modern and ever advancing cyber threats.
- Complexity of healthcare systems with numerous sub-systems and stakeholders, creating multiple points of vulnerability (5);
- The shortage of expertise on digital technology and cybersecurity in health systems challenges effective cyber incident prevention and response.

- The absence of comprehensive cybersecurity policies exposes health data to unauthorized access at both individual and aggregate levels (6).

Despite evident risks and increasing expectations for privacy compliance, many health systems overlook cybersecurity and privacy protection mechanisms in their strategy and investments. The Check Point Research half-year report for 2023 (7) highlights a significant increase in the frequency and volume of cyber-attacks against the health sector in recent years. Cyber-attacks on health systems can disrupt critical health services. This disruption erodes clients' trust due to unauthorized access to private information and hindered access to health services, potentially resulting in adverse health outcomes (8). For example, compromised electronic health records or manipulated medical data from a cyber-attack could lead to misinformed clinical decisions, delayed treatments, or even the administration of incorrect medications - emphasizing the need for robust cybersecurity measures to safeguard, not only data, but also the lives and well-being of individuals (9).

Cybersecurity is beyond a technical concern, but a health and safety concern. Dedicated budgetary support for cybersecurity and privacy protection allows for better preparedness and agility in responding to cyber-attacks (10), (11).

Regulatory frameworks also play a pivotal role in setting stringent requirements for patient data protection e.g., Health Insurance Portability and Accountability Act (HIPAA)(12) and, General Data Protection Regulation (GDPR) (3). Staying informed of emerging threats, continuously implementing risk mitigation mechanisms, adopting cybersecurity practices like encryption and multi-factor authentication, adopting contingency plans and processes, promoting collaboration, and educating stakeholders can support a health system against evolving cyber challenges.

3. Use cases for cybersecurity, confidentiality, and privacy.

3.1 Person-centered data management

Person-centered care requires a paradigm shift in health systems to allow for health data to follow an individual through their continuum of care, often requiring data to be shared across multiple health workers, health facilities, and multiple health service providers. The heightened need for multiple stakeholders to access health data across multiple sources for quality service delivery, introduces greater complexity in ensuring that health data is shared in a secure and privacy protecting manner. Secure health systems interoperability enables the continuous provision of care across independent interoperable health service providers, enhancing quality of care. Safe, seamless, secure, and confidential information sharing across all healthcare providers using global interoperability standards must be guaranteed for the data exchange to be trusted.

3.2 Cross-Jurisdiction verification of health documents

With the significant number of migrants and individuals who travel internationally, it is critical to ensure people can have access to their health information regardless of where they are. A mechanism for enabling verification of health information and health documents across jurisdictions is the use of a Trust network (13), which facilitates exchange of data in a secure and trusted manner to give an assurance of privacy and confidentiality. It is essential to safeguard these networks from cyberattacks to enable secure cross-jurisdictional data sharing.

3.3 Security and privacy in medical devices

Cybersecurity and privacy must be actively managed over the intended life cycle of a medical device, from design through installation, use and decommissioning. The increased use of Internet of Things (IoT) in health makes this imperative more acute. There are situations where usability of medical devices may extend beyond their intended use or End of Life (EoL) or End of Support (EoS). Such devices, termed as legacy devices, are no longer able to receive critical updates, including cybersecurity updates and patches. Even though the benefits of using a legacy device may be determined to outweigh the risks, the risks should never be overlooked, as legacy devices may be more vulnerable to cyberattacks, and interconnected legacy devices can spread malware and ransomware to other systems. Additionally, legacy devices may not provide an adequate level of privacy protections for patients and other stakeholders. To establish medical device cybersecurity protocols, guidance from organizations such as the International Electrotechnical Commission (IEC) and the International Medical Device Regulators Forum (IMDRF) should be adhered to.

4. Implementing resilient and secure digital health systems

For secure, person-centered digital health systems, essential factors include having a shared understanding of cybersecurity and privacy among key stakeholders, such as ministries of health and ministries of ICT. Implementing of digital health systems as part of a digital health intervention requires adopting a *security and privacy by design* approach, embedding principles and requirements in the design stage, and throughout the entire intervention's lifecycle. Several information security and cybersecurity frameworks exist and can be referenced for this process, such as NIST CSF (2), National Institute of Standards and Technology Risk Management Framework NIST RMF (14), Control Objectives for Information Technologies COBIT (15), International Organization for Standardization/International Electrotechnical Commission ISO/IEC 27001/2 (16), Federal Information Security Management Act FISMA (17), General Data Protection Regulation GDPR (3), Health Insurance Portability and Accountability Act HIPAA (12), Payment Card Industry Data Security Standard PCI DSS (18) and Coordinated Healthcare Incident Response Plan CHIRP (19). Implementing secure systems not only requires preventing cybersecurity incidents, but also effectively containing, responding, and recovering from them. Patient safety is a critical concern during incident response. Figure 1 summarizes the eight steps for implementing secure, person-centered digital systems.

4.1 Demonstrate top-level cybersecurity and privacy commitment.

Top management in ministries of health, ministries of ICT, and ministries of finance need to support the efforts towards cybersecurity and privacy protection, which may be driven by a multisectoral steering committee. The checklist below summarizes key questions to indicate sufficient top-level management commitment.

Top management commitment checklist

Awareness creation among the policy makers

- Are public and private healthcare providers' cybersecurity strategies aligned with the MoH objectives for cybersecurity, patient safety, confidentiality, and privacy of digital health systems? *If not, see, Organization for Economic Co-operation and Development (OECD)* (20), *National eHealth Strategy Toolkit by WHO* (21)*, GDPR*(3)*.*

- Has cybersecurity and privacy protection in health been incorporated into the country's whole-of-government information technology risk management? *If not, see: NIST* (2), *COBIT* (15)*, NIST Special Publication NIST SP 800-53* (22)*.*

Commitment to investment

- Is there commitment by the different ministries' leadership to providing adequate resources to support cybersecurity and privacy risk management for digital health systems? *If not, see: European Union Agency for Cybersecurity ENISA's Report on Cybersecurity Investments, ROSI* (23)
- Are there relevant cybersecurity and privacy protection committees or advisory groups, composed of relevant ministries and key partners to address governance, regulatory, compliance, technical, and logistical aspects? *If not, see: National Initiative for Cybersecurity Education NICE Framework*(24)*, ENISA Skills Framework* (25).

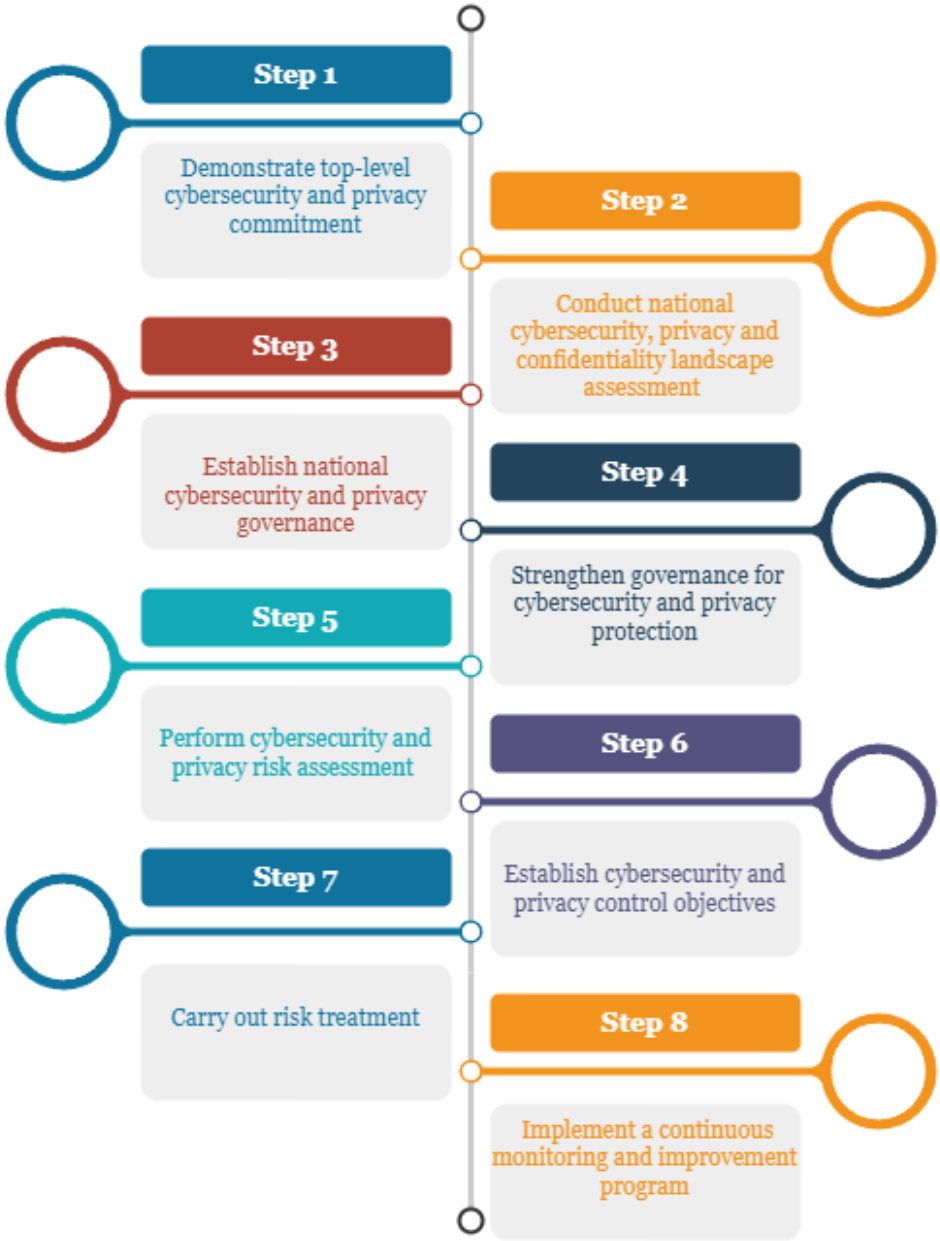

Figure 1: Stepwise approach to implementing resilient and secure digital health systems.

4.2 Conduct national landscape assessment

Understanding what assets need to be secured and what information needs to be protected is a critical part of a landscape assessment. Assessing the supply chain landscape is also crucial for understanding risks from suppliers, service providers and other active actors involved in delivery of digital health systems to safeguard retrogression. Further, frameworks like *Capability Maturity Model Integration (*CMMI) (26), Cybersecurity Capability Maturity Model (C2M2) (27) , and CMM (28) help determine cybersecurity maturity levels and establish benchmarks for risk reduction. This initial landscape assessment helps guide investments and activities.

Landscape assessment checklist

National health data and information assets

- Is the current cybersecurity and privacy context and maturity level of the country established? *If not, see: National Cybersecurity Index NCSI* (29)*,* CMM (28)*, CMMI* (26), *C2M2* (27)
- Has an inventory of all health information assets (software, hardware, people, data) been carried out and their related cybersecurity and privacy risks been assessed? *If not, see: NIST Guide for Conducting Risk Assessments NIST GCRA* (30)*, Operationally Critical Threats, Assets and Vulnerability Evaluation OCTAVE* (31)*, NIST-CSF*(2)*.*
- Have third party vendors, suppliers and service providers been assessed to determine their cybersecurity maturity levels? *if not, see: CMM*(28)*, CMMI* (26)*, C2M2*(27)*, NIST Risk Management Framework NIST-RMF* (14)*.*

Policies and governance

- Is there legislation about how health information should be collected, stored, accessed, and shared? *If not, see: Cyber Strategy and Development Framework CSDI* (32)*.*
- Is there legislation about hosting citizens' health data records outside of the country (including individual level or aggregate data)? *If not, see: CSDI* (32)*.*
- Is there a national Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) that publishes cybersecurity Coordinated Vulnerability Disclosures with mitigations and compensating controls? *If not, see: National Cyber Security Strategy Good Practice Guide NCSSGPG* (33)

Public awareness and communication

- Is the public aware of cybersecurity and data privacy concerns and their rights over their health data? *If not, see: NCSSGPG* (33)
- Are cybersecurity threats and vulnerabilities communicated for maximum awareness and response? *If not, see: NCSSGPG* (33)
- Have the necessary cybersecurity and privacy policies been determined, established, and communicated to stakeholders? *If not, see: Centre for Internet Security CIS* (34)*, COBIT* (15)*, NIST-CSF* (2)

4.3 Establish national cybersecurity and privacy protection goals.

Once a national landscape assessment has been carried out, a risk management strategy should then be formulated to advance the country's cybersecurity maturity. The risk management strategy is important when building a robust cybersecurity program to identify, assess, prioritize, and mitigate potential risks proactively. To comprehensively conduct this assessment, the checklist below includes key questions and references to facilitate the process.

National cybersecurity and privacy goals checklist

- Have the national cybersecurity and privacy goals been set? Are they aligned with the country's strategic direction? *If not, see:* National Capabilities Assessment Framework *NCAF* , *NCSSGPG* (33)
- Has a comprehensive national cybersecurity strategy that outlines the country's goals, priorities, and actions for securing cyberspace been developed? *If not, see: NIST-CSF* (2), *CIS* (34), *ENISA*(23) , *Digital Security Risk Management for Economic and Social Prosperity by Organization for Economic Co-operation and Development OECD* (35)
- Has the Ministry of Health determined a cybersecurity and privacy risk management strategy, and established relevant policies? *If not, see: NIST SP 800-37* (22), *ISO 31000:2018* (36) *Risk management guidelines.*
- Where health services and assets are accessed at home by clients or by mobile healthcare workers, has a risk management strategy been established for them? *If not, see: NCSSGPG* (33), *Health Industry Cybersecurity Matrix of Information Sharing Organizations HIC-MISO* (37)

4.4 Strengthen governance for cybersecurity and privacy protection.

Governance is required to support policies and processes for ensuring effective oversight of cybersecurity and privacy protection initiatives. It involves defining roles, responsibilities, mechanisms for monitoring, evaluating, and regulating cybersecurity measures. Cross-sectoral collaborative efforts across health, legal, and ICT domains are integral. Despite challenges in local or international interoperability, cybersecurity and privacy governance plays a significant role to support secure data exchange. Aligning regulatory frameworks with cybersecurity needs is vital to support construction and use of secure digital health systems. Regular assessments of effectiveness of cybersecurity and privacy management activities are also needed to ensure documentation and formal communication of changes in the regulatory landscape, feedback from monitoring and evaluation. The checklist below outlines key questions to guide the establishment of governance of cybersecurity and privacy protection.

Governance strengthening checklist.

National cybersecurity legal framework

- Does national cybersecurity and privacy legislation exist, together with policies, strategies, and guidelines to support its implementation at various levels of the healthcare system? *If not, see: ENISA* (23), *GDPR* (3), *CIS* (34)*Critical Security Controls.*
- Have cybersecurity and privacy laws and regulations been enacted to address emerging threats and technologies, as well as requiring the reporting of cybersecurity incidents, ensuring a coordinated response and information-sharing mechanism? *If not, see: HIPAA* (12), *ENISA* (23), *GDPR* (3), *CIS* (34) *Critical Security Controls, National eHealth Strategy Toolkit by WHO* (21).
- Is there a mechanism to enforce robust cybersecurity, data protection and privacy laws to safeguard citizens' personal information? *If not, see: ENISA* (23), *GDPR* (3), *Asia-Pacific Economic Cooperation APEC* (38) *Privacy Framework, CIS* (34) *Critical Security Controls.*
- Are there legal provisions for clients to provide informed consent for the collection, use, and sharing of their health data? *If not, see: ENISA* (23), *GDPR* (3).
- Are there legal provisions for patients to have the right to access their own health records? *If not, see: ENISA* (23), *GDPR* (3)
- Is there a predetermined schedule for regular reviews that is aligned to the risk management program? *If not, see: NIST-CSF* (2), *COBIT* (15), *NIST SP 800-53* (22).

Governance and feedback

- Are there defined governance structures to oversee countrywide cybersecurity and privacy efforts in health data systems? *If not, see: ISO/IEC 27001* (16)*, ISO/IEC 27701* ,(39) *NIST-CST* (2)*, NIST SP 800-53* (22)*, COBIT* (15).
- Is there a governance mechanism to support identification and prioritization of cybersecurity countermeasures? *If not, see: : NIST-CSF* (2)*, COBIT* (15)*, CIS* (34) *Critical Security Controls.*
- Is there accountability among top-level management that would ensure cybersecurity and privacy risks are adequately mitigated, along with KPIs for risk mitigation? *If not, see: NIST-CSF* (2)*, COBIT* (15)*, CIS* (34) *Critical Security Controls, ISO 31000:2018* (36).
- Have cybersecurity and privacy roles and responsibilities been established and aligned with the policies, legal and regulatory framework? *If not, see CIS* (34) *Critical Security Control, NIST-CST* (2)*, NIST SP 800-53* (22)*, COBIT* (15).
- Is there a feedback mechanism to top leadership in the Ministry for current cybersecurity status, recommendations on continuous improvement, and suggestions for change in national policies, laws, and regulations? *If not, see NIST-CST* (2)*, NIST SP 800-53* (22)*, COBIT* (15)*, NIST SP 800-37* (40) .

Capacity building and awareness

- Is there a mechanism for promoting capacity building in cybersecurity and privacy with short term and long-term training, awareness, innovation, and research? *If not, see: NICE Framework* (24)*, ENISA Skills Framework* (25)*, CMM* (28).
- Is there a provision for public awareness campaigns to educate citizens about the importance of cybersecurity, data privacy, and how to protect their health information? *If not, see: Digital Security Risk Management for Economic and Social Prosperity OECD* (35)*, Empowering a more secure, interconnected world by the National Cybersecurity Alliance NCA* (41).
- Is there an ongoing security awareness training program for all healthcare provider staff and patients? *If not, see: ISO/IEC 27001* (16)*, NIST-CSF* (2)*, GDPR* (3).

Collaboration and resource allocation

- To achieve cross-border interoperability, has the country established agreements or mechanisms for secure cross-border transfer of health data, addressing issues related to data sovereignty and privacy? *If not, see: GDPR* (3)*, ENISA* (23)*, APEC* (38)*, CIS* (34)
- Is there a budget to support preventative activities and incident response? *If not, see: ENISA report on cybersecurity investments* (42)*,* Return on Security Investment *(ROSI)* (23)
- Where governance spans more than one institution, is there a framework to mitigate budgetary and logistical risks? *If not, see: OECD Recommendation* (20) *on Health Data Governance, COBIT* (15)*, ENISA report on cybersecurity investments* (42).

Support for conformance

- Is there a national data protection regulator charged with protecting the privacy rights of citizens and organizational compliance to privacy law? *If not, see: NICE Framework* (24)*, GDPR* (3).
- Is there an agency or department charged with the responsibility of coordinating the country's cybersecurity, with skills and resources to oversee the governance and policy environment? *If not, see: NICE Framework* (24).

4.5 Perform cybersecurity and privacy risk assessment.

Risk assessment entails identification of the specific systems and assets, including data, which need to be protected, the possible threats they may be exposed to, the potential impact, the likelihood of an incident happening, and the risk acceptance criteria. Performing a risk assessment begins with defining a risk assessment process that ensures consistent and repeatable outcomes. Thereafter, the country should establish risk prioritization as guided by NIST IR 8286 to inform risk mitigation activities. Cybersecurity and privacy risk assessment may be conducted together or may form two separate but related processes that may be run in parallel or independent of each other.

A risk assessment is not only performed on the digital applications, but it is also performed on the overall architecture and infrastructure (or platform) that hosts the application and data processing activities, the people involved in the process, and on the governance mechanism in place that guide the standard operating procedures.

Risk assessments should be done periodically, based on the defined process, or when necessary, such as when there is an update to the digital health systems or knowledge of an emergent cyber threat. Performing risk assessments are important for stakeholders to identify, estimate and prioritize risks faced.

In cases where a third party is involved in providing health data systems or related services, whether from another government entity, facilitator organization, development partner or commercial entity, the third party should fill a cybersecurity and privacy questionnaire (see Annex 4). This security questionnaire should then be analyzed with the purpose of determining if the third party is compliant with the required level of security relating to the product, people, and processes of their organization, or what is required of them to reach the required level of compliance. Should it be determined that the third party is below the required level, then, the Ministry should assess whether they can be required to upgrade and meet the requirements. There may be cases where the impact of not implementing the product outweighs the risk of compliance of the third party. In such cases, the Ministry should be intentional in deciding a path forward and make necessary adjustments with appropriate documentation. The checklist below outlines key questions to support the development of a risk assessment mechanism.

Risk assessment checklist

Risk assessment and management

- Are sound risk assessment plans established with relevant criteria and metrics? *If not, see: NIST-CSF* (2)*, COBIT* (15)*, NIST SP 800-30* (30)*, a Guide for Conducting Risk Assessments.*
- Have the major risks of the health information system and digital health architecture been identified and prioritized? Has cybersecurity and privacy management process been established? *If not, see: Information security management systems ISO/IEC 27001* (16)*, COBIT* (15)*, The Privacy, Confidentiality and Security Assessment Tool by the United Nations Program on HIV/AIDS UNAIDS* (43)*, OCTAVE* (31)*.*
- Has risk tolerance been determined, justified, and prioritized? *If not, see: NIST-CSF* (2)*, COBIT* (15)*.*
- Do we have fit-for-purpose risk escalation flows that will ensure detection and trigger remediation/mitigation? *If not, see: NIST-CSF* (2).
- Is there a cybersecurity risk management and vulnerability management plan for medical devices in use? *If not, see: Principles and Practices for the Cybersecurity of Legacy Medical*

Devices by the International Medical Device Regulators Forum IMDRF (44)*, Medical Device and Health IT Joint Security Plan* (45), Health Industry Cybersecurity – Managing Legacy Technology Security *HIC-MaLTS* (46).

Personnel, skills, and competence

- Are there local ministry staff with the required skill set for cybersecurity and data privacy to govern, identify, protect, detect, respond, and recover from threats as described in NIST Cybersecurity Framework? *If not, see: NIST-CSF* (2).
- Are there background verification processes for all staff during onboarding? *If not, see: ISO/IEC 27001* (16).
- Are all healthcare staff competent and aware of their responsibilities as defined in cybersecurity, privacy, and related policies? *If not, see: NIST-CSF* (2).
- Do we have suitable, qualified professionals with adequate expertise in cybersecurity and privacy to perform risk assessments? *If not, see: ISO/IEC 27001* (16)*, COBIT* (15).
- Are there local partners with CMMI maturity level of five to provide secure system implementations? *If not, see: CMMI* (26).
- Is there a team specifically dedicated to protecting, monitoring, and responding to cybersecurity and privacy of health data systems and networks? *If not, see: NIST-CSF* (2)*, COBIT* (15).

Data, systems, and network protection

- Is there a team in charge of access, authorization, anonymization, and curation of health data? *If not, see: NIST-CSF* (2)*, COBIT* (15).
- Have all outsourced processes and systems from third party vendors been determined? *If not, see: ISO/IEC 27001* (16)*, COBIT* (15)*, Vendor Risk Assessment Template* (47)
- Are there notices provided to users of medical devices on data collection, storage, and use of personal data? *If not, see: HIPAA* (12).
- Have the risks associated with medical devices in use that no longer receive security updates been determined? *If not, see: IEC 81001-5-1:2021* (48) *, Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook* (49).
- What data is being stored and/or transmitted on or between medical devices and other systems and how is it being protected? *If not, see: Medical device and health IT joint security plan* (45).

4.6 Establish cybersecurity and privacy control objectives.

This step involves defining cybersecurity and privacy control objectives that are measurable and aligned with the cybersecurity and privacy goals and risk assessment results. Control objectives are the activities to be conducted to achieve secure digital health systems. In addition to setting the control objectives, this step also involves determining who will be responsible, what resources will be needed, when to complete the objectives, and how the results will be evaluated. The set control objectives will need to be monitored, measured, and evaluated using appropriate key performance indicators (KPIs) and metrics to assess their effectiveness towards cybersecurity. It is important to align the control objectives with relevant regulations of the country and, where necessary, in the region support security and privacy of data. Examples of privacy controls include HIPAA in the U.S. and GDPR in Europe. The checklist below provides the necessary questions to guide in setting appropriate cybersecurity and privacy control objectives.

Control objectives establishment checklist

Objectives setting and planning.

- Are the objectives specific, measurable, achievable, relevant, time-bound? Are plans to achieve the objectives established, assigned to process owners, budgeted for, and scheduled? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39)*, and COBIT* (15)*, Guidelines on protecting the confidentiality and Security of HIV information by UNAIDS* (50)*.*
- Have the resources, including budget and personnel, required to achieve each control objective been provided? *if not, see: NICE Framework* (24).
- Are cybersecurity and privacy specific objectives established and aligned with the country's unique requirements in health data systems and the cybersecurity and privacy requirements and overall risk assessment results? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39)*, NIST SP 800-30* (30), *GDPR* (3)*.*
- Do the cybersecurity and privacy control objectives match with the country's risk tolerance? If not, see: *: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39), and *COBIT* (15).
- Is there a process for ensuring ongoing compliance with applicable laws and regulations? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39)*, NIST SP 800-30* (30), *GDPR* (3)*.*
- Is privacy by design integrated into the development of new systems and processes from the outset, to minimize the collection and storage of personal information to what is strictly necessary and to obtain and manage user consent for the collection and processing of personal information? *If not, see: GDPR* (3)*, Privacy by Design* (51) *principles, ISO/IEC 27701* (39).
- Do control objectives address the security and privacy practices of external vendors and partners? *If not, see: : NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39)*, NIST SP 800-30* (30)*.*

Cybersecurity and privacy governance

- Are there defined governance structures to oversee cybersecurity and privacy efforts? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39)*, NIST SP 800-30* (30)*, COBIT* (15)*.*

Monitoring and evaluation of control objectives

- Is there a program for regular audits of cybersecurity and privacy controls? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, ISO/IEC 27701* (39)*, NIST SP 800-30* (30)*, COBIT* (15)*.*

- Is there a mechanism to measure and monitor the effectiveness of the control objectives? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, COBIT* (15).
- Is there a plan to regularly review and update control objectives based on evolving threats and changing organizational needs? *If not, see: NIST-CSF* (2)*, ISO/IEC 27001* (16)*, COBIT* (15)*.*

4.7 Carry out risk treatment.

Risk treatment involves creating a plan for managing identified risks through risk mitigation, risk avoidance, and risk transfer in the cybersecurity and privacy process. Risk treatment begins with defining a process, implementing security controls, and conducting ongoing stakeholder training. The risk treatment process should be based on risk assessment results, documenting controls, and justifying inclusions or exclusions to mitigate, avoid, or transfer risk.

Examples of risk treatment include implementing necessary security controls that protect assets such as authentication, encryption, staff awareness training, encryption for data in transit and at rest, anti-virus software, keeping all software updated. Ongoing training and awareness of key stakeholders and the public have been reported to be major contributors to cybersecurity. By sensitizing staff and the public of the dangers and how to avoid and respond appropriately, the likelihood of successful attacks is minimized. The dynamic nature of threat landscapes demands that training and awareness be ongoing activities (52).

Implementing and operationalizing all necessary cybersecurity and privacy controls is crucial, considering that different electronic systems face varying threats and require tailored risk treatments, ensuring alignment with existing compliance requirements. In addition to protecting the system, it is important to have a well-defined incident response plan in place. This plan should outline the steps to be taken in the event of a cybersecurity incident, including reporting, containment, and recovery procedures. That way, when an incident does occur, the response plan can be readily used and followed to apply the necessary control actions, and therefore mitigate the risk.

When establishing incident response and risk treatment processes, the person or entity responsible for managing and mitigating the specific risk - termed as the "*risk owner*" - should be involved. The risk owner understands the risk well and has the authority to do something about it, implementing controls, and monitoring the risk over time.

Risk treatment checklist

Risk treatment planning

- Are risk treatment and incident response processes established, with all relevant risk owner approvals, which outlines the steps to be taken in the event of a security incident and the response roles and responsibilities clearly defined? *If not, see:* NIST CSF (2), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53), *NIST SP 800-53* (22), *NIST.SP.800-61* (54), *ISO/IEC 27001* (16), *ISO/IEC 27701* (39).
- Is there a mitigation response for every possible high-risk incident? *If not, see:* NIST CSF (2), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53), *NIST SP 800-53* (22)
- Is there a well-defined incident response plan that aligns with control objectives? *If not, see:* NIST CSF (2), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53), *NIST SP 800-53* (22), *NIST.SP.800-61* (54), NIST-RMF (14)
- If legal requirements for healthcare organizations are to notify patients and authorities in the event of a data breach, have all notifications been done? *If not, see:* *GDPR* (3), *HIPAA* (12).
- Has the organization developed a consistent, repeatable process for communicating identified cybersecurity threats, incidents, and vulnerabilities in a timely manner, along with clear actions for reducing risk? *If not, see:* *ISO/IEC 27002* (53), *NIST.SP.800-61* (54), *NIST-CSF* (2), *ISO/IEC 27001* (16).

Standards and compliance

- Are there standards or blueprints on the required setup of hosting environments running sensitive data systems? *If not, see:* , *ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Are there cybersecurity and privacy standards regarding the levels of encryption? *If not, see:* , *ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Are there standards for anonymization of personally identifiable information? *If not, see*, *ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Are there standards governing the minimum requirements on service levels of hosted health records data systems? *If not, see:* , *ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Are there standards governing the minimum requirements on service levels of health records data on transit? *If not, see:* , *ISO/IEC 27002* (53), *NIST SP 800-53* (22).

Access controls and user management

- Are physical and logical access controls in place to access health systems and data both at rest and in transit? *If not, see:* , *ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Are Role-Based Access Controls applied and documented in all health data systems alongside the user accounts? *If not, see:* , *ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Are user accounts reviewed periodically for unauthorized use or access? *If not, see: NIST CSF* (2), (2), CIS (34) Critical Security Controls, *ISO/IEC 27001* (16).

Security measures and countermeasures

- Have all appropriate controls been applied to protect the prioritized risks? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22), CIS (34) Critical Security Controls.
- Are all countermeasures such as intrusion detection systems, anti-virus, etc., regularly reviewed and kept up to date? *If not, see ISO/IEC 27002* (53), *NIST SP 800-53* (22), CIS (34) Critical Security Controls.
- Are there measures in place to ensure the confidentiality, integrity, and availability of health data in transit and at rest? *If not, see: ISO/IEC 27001* (16), *NIST-CSF* (2), *NIST SP 800-53* (22).
- Are data encryption mechanisms implemented for sharing sensitive information? *If not, see: ISO/IEC 27001* (16), *NIST-CSF* (2), *NIST SP 800-53* (22), *ISO/IEC 27002* (53).
- Are there controls in place to manage the lifecycle of software and hardware assets, including their acquisition, operation, retention, and disposal? *If not, see: ISO/IEC 27001* (16), *NIST-CSF* (2), *COBIT* (15).
- Have best practices to help safeguard medical devices in use been established? *If not, see: Medical device and health IT joint security plan* (45).
- Are there controls in place to secure medical devices that are used beyond End of Life (EoL) or End of Support (EoS)? *If not, see: HIC-MaLTS* (46), *Medical Device and Health IT Joint Security Medical device and health IT joint security plan* (45).
- Are all software and hardware assets up to date and with the latest security updates and patches, including medical devices? *If not, see: NIST-CSF* (2), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53), *Medical device and health IT joint security plan* (45), *HIC-MaLTS* (46).
- Is there a business continuity and disaster recovery plan in place to ensure the availability and integrity of health data in case of emergencies? *If not, see: NIST-CSF* (2).
- Are firewalls and intrusion detection/prevention systems in place and updated? *If not, see:* CIS (34) Critical Security Controls.

Contractual and operational safeguards

- Are confidentiality agreements applied when handling confidential information? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Is there a service level agreement with critical health data systems service providers? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22).
- Does the software development lifecycle, whether in-house or outsourced, embed secure software development best practices? *If not, see ISO/IEC 27002* (53), *NIST SP 800-53* (22), CIS (34) Critical Security Controls
- Have all outsourced third-party processes and systems been documented, assessed, and controlled? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22), *NIST.SP.800-61* (54).

Incident response and recovery

- Is there a communication and reporting mechanism for all attacks? *If not, see ISO/IEC 27002* (53), *NIST SP 800-53* (22), CIS (34) Critical Security Controls, *NIST.SP.800-61* (54).
- Are health data systems backups kept up to date? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22), *NIST.SP.800-61* (54), CIS (34) Critical Security Controls.
- Is there a timely restore mechanism for all scenarios? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22), *NIST.SP.800-61* (54), CIS (34) Critical Security Controls.
- Are health data systems backups ready for immediate recovery? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22), CIS (34) Critical Security Controls.
- Are changes to planned implementations of cybersecurity controls documented? *If not, see: : ISO/IEC 27002* (53), *NIST SP 800-53* (22), *NIST.SP.800-61* (54), CIS (34) Critical Security Controls.
- Are there automated threat detection mechanisms? *If not, see: NIST-CSF* (2), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53).

Alignment with ministry objectives and privacy

- Does the treatment plan align with the ministry's objectives in supporting the identification and prioritization of actions for reducing cybersecurity risks? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22), CIS (34) Critical Security Controls.
- Are regular cybersecurity and privacy general awareness training conducted as well as training for specialized cybersecurity staff? *If not, see: ISO/IEC 27002* (53), *NIST SP 800-53* (22).

Privacy compliance

- Are there defined processes and responsibilities in place to honor and fulfil privacy rights requests? *If not, see: ISO/IEC 27701* (16), *GDPR* (3), *NIST.SP.800-61* (54).
- Have minimum and maximum retention periods been defined for personal datasets? *If not, see: ISO/IEC 27701* (16), *GDPR* (3), *NIST.SP.800-61* (54).
- Are there mechanisms in place to provide confidential information to users of the digital health system? *If not, see: ISO/IEC 27701* (16), *GDPR* (3).

4.8 Implement a continuous monitoring and improvement program.

Continuous monitoring includes determining what, how, and when to monitor, linking monitoring with risk treatment plans for swift countermeasures when threats arise. Remaining vigilant ensures constant awareness of incidents, vulnerabilities, and security status. Automated monitoring through various tools such as artificial intelligence (AI), managed Network Detections and Response (NDR) tools as well as Extended Detection and Response (XDR) tools enhance accuracy and efficiency in scanning for cyberattacks and compliance. Combining automated tools with supervised monitoring allows authorized security officers to make informed risk-based decisions. The monitoring should be comprehensive enough to include the monitoring of user behavior. For example, monitoring behavioral patterns and aspects of users to model proper use of health data systems and thereby detect misuse. AI driven anomaly detection technologies can be leveraged to achieve this.

Maintaining comprehensive documentation is crucial. A dedicated Security Operation Centre (SOC) or integration of health data systems into existing SOC surveillance systems can enhance monitoring capabilities. Continuous improvement, guided by regular internal audits, helps address identified gaps by reviewing nonconformities and adjusting cybersecurity and privacy controls. This improvement cycle should remain intricately linked to the monitoring program to adapt to system changes, evolving threats, and varying risk tolerances.

Performing internal and external audits for continuous monitoring and improvement is key. This involves conducting audits to assess compliance with cybersecurity and privacy standards for patient-centered digital health data systems. An audit plan should be established, specifying frequency, methods, responsibilities, and reporting, with impartial auditors engaged for objectivity. For third-party vendors, a vulnerability assessment is recommended during onboarding, using templates like Up guard's Vendor Risk Assessment (47). Privacy audits of vendors ensure data processing protection. External audits are advised, with certified third-party cybersecurity audit firms. Vulnerabilities identified in audits should be promptly addressed, and a fresh audit conducted. Internal audits before major system changes and continuous monitoring, coupled with regular security audits, help detect and address vulnerabilities and potential breaches. Subsequent maturity assessments may follow a successful external audit.

Continuous monitoring and improvement checklist

Monitoring

- Is continuous monitoring of all health systems, data and networks conducted? *If not, see: NIST - Information Security Continuous Monitoring ISCM* (55), *NIST-CSF* (2), *ISO/IEC 27001* (16), *NIST.SP.800-61* (54).
- Has a mechanism to continuously maintain an up-to-date inventory of all health information assets been established? *If not, see: NIST-CSF* (2), *COBIT* (15), *ISO/IEC 27002* (53).
- Is cybersecurity self-assessment regularly carried out? *If not, see: NIST-CSF* (2), CIS (34) Critical Security Controls, *ISO/IEC 27001* (16).
- Does the continuous monitoring program support monitoring of regular cybersecurity and privacy general awareness training for specialized cybersecurity staff? *If not, see: NIST-CSF* (2), *COBIT* (15), *ISO/IEC 27001* (16).
- Is there a process that monitors data subject requests and keeps track of whether they are addressed in a timely manner, in line with regulatory requirements? *If not, see NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), *NIST.SP.800-61* (54).
- Is there a process for regularly reviewing and updating third-party risk assessments for continuous improvement of risk mitigation and monitoring activities? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), *NIST.SP.800-61* (54).
- Are processes and procedures on the security and retention of audit logs established? *If not, see: see NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), *NIST.SP.800-61* (54).
- Is cybersecurity self-assessment routinely carried out to continue to improve risk identification, mitigation, and monitoring? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53), *NIST.SP.800-61* (54).

Improvement

- Have the existing cybersecurity policies and guidelines been assessed for necessary improvement based on lessons learned as well as from predictive indicators? *If not, see: NIST-CSF* (2), *COBIT* (15), *ISO/IEC 27001* (16), *NIST.SP.800-61* (54).
- Are cybersecurity and privacy controls regularly reviewed for improvement? *If not, see: NIST-CSF* (2), *COBIT* (15), *ISO/IEC 27001* (16), *NIST.SP.800-61* (54).
- Is continuous improvement embedded in the performance of stakeholders? *If not, see: NIST-CSF* (2), *COBIT* (15), *ISO/IEC 27001* (16), *NIST.SP.800-61* (54).
- Are regular testing and simulation exercises conducted for their incident response plans? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), CIS (34) Critical Security Controls, *ISO/IEC 27002* (53).

Auditing

- Are internal audits scheduled at least twice a year and for when system updates are carried out? *If not, see: COBIT* (15), *ISO/IEC 27001* (16) , *ISO/IEC 27002* (53).
- Are external audits scheduled to take place on a regular basis, at least once a year? *If not, see: COBIT* (15), *ISO/IEC 27001* (16) , *ISO/IEC 27002* (53).
- Does the onboarding process of external service providers and third parties include a cybersecurity audit? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), CIS (34) Critical Security Controls.
- Is there a mechanism to ensure that audit findings are communicated to management in a timely manner? *If not, see: COBIT* (15), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), *NIST.SP.800-61* (54).
- Do auditing processes incorporate measures to verify and validate the effectiveness of implemented controls? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), CIS (34) Critical Security Controls.
- Is there evidence of policy adherence? *If not, see: ISO/IEC 27001* (16) , *ISO/IEC 27002* (53), *IT Audit Framework ITAF* (56), *COBIT* (15).
- Are physical and system access controls in place for systems, applications, and data and is it reviewed and aligned with job responsibilities? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), CIS (34) Critical Security Controls, *ITAF* (56), *COBIT* (15),
- Does the auditing process identify whether the incident response plan undergoes regular testing? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), CIS (34) Critical Security Controls, *ITAF* (56), *COBIT* (15), *NIST.SP.800-61* (54).
- Are incidents logged, investigated, and documented? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), CIS (34) Critical Security Controls, *COBIT* (15), *NIST.SP.800-61* (54).
- Does the auditing process include an audit of the security awareness training program for employees for relevance and adequacy? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), CIS (34) Critical Security Controls, *ITAF* (56), *COBIT* (15).
- Are risk assessments conducted regularly? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), CIS (34) Critical Security Controls, *ITAF* (56), *COBIT* (15).
- Are critical systems and data regularly backed up and restorable? *If not, see: NIST-CSF* (2), *ISO/IEC 27001* (16), *ISO/IEC 27002* (53), CIS (34) Critical Security Controls, *COBIT* (15).
- Is identity and access management periodically reviewed? *If not, see: ISO/IEC 27001* (16), *ISO/IEC 27002* (53), CIS (34) Critical Security Controls, *ITAF* (56), *COBIT* (15).

5. Budgeting for cybersecurity, data confidentiality and privacy

A comprehensive cybersecurity budget is increasingly becoming a national priority as countries increasingly adopt digital health systems. However, budgeting for cybersecurity has usually been ad hoc and reactive. A risk-based approach is a proactive budgeting approach that considers risk tolerance and risk mitigation measures across several domains. This enables a country to prioritize investment in areas that will make a noticeable improvement to their information security operations.

There is no universally agreed amount or percentage of a country's overall budget that should be allocated to cybersecurity or privacy protection. Each country is at a different level of cybersecurity maturity with different economic capacity and specific priorities. Any enterprise looking to implement

cyber defenses is required to know three things: Which protections to start with; Which tools will be needed to implement those protections? and how much will an implementation cost? Further, the allocation of budget should be flexible enough to support the recovery activities should a cybersecurity breach occur, as it is often a question of "when" a cyber-attack would happen rather than a question of "if" a cyber-attack would happen (57).

To budget effectively in the unpredictable realm of cybersecurity, justifying investments becomes crucial. The Return on Security Investment (ROSI) method, proposed by ENISA, provides a formal and quantitative risk assessment solution. ROSI method is a flexible and fit-for-purpose method that can be applied to any organization, sector, or sustainability effort. This method aids in identifying cost-effective cybersecurity solutions, determining suitable investment amounts, and evaluating the impact on overall productivity. The ROSI method entails five steps that include: understand the business model; identify key assets; set the foundation; make a scenario-plan; and quantify the risk and identify controls. In its basic form, ROSI involves estimating the Annual Loss Expectancy (ALE), representing the potential monetary loss, and comparing it with the cost of the proposed countermeasure. The formula is as follows:

$$ROSI = \left(\frac{Annual\ Loss\ Expectancy - Cost\ of\ the\ proposed\ countermeasure}{Cost\ of\ the\ proposed\ countermeasure}\right)$$

ROSI's adaptability makes it suitable for various priorities and scenarios. For instance, when choosing among different countermeasures, such as firewalls with documented estimates of their effectiveness, incorporating this measure into the ROSI equation provides a more accurate estimate of return on investment. The effectiveness of the countermeasure plays a crucial role, especially when the potential monetary loss is high. Loss, in a health context, however, is not limited to monetary terms; it can include loss of trust, goodwill, personal privacy, negative health outcomes, or loss of life. ROSI framework accommodates techniques to compute losses including loss of life such as Demographic method; Statistical evaluation; Actuary approach method; and Legal approach. To examine potential loss or exposure, organizations should take a detailed look at the threat landscape, attack surface and business model in a particular environment. Acquisition of necessary data is key when estimating potential loss for both tangible and intangible assets. Data helps in understanding the key actions to take and know where a firm stands on its cyber risk journey.

5.1 Key steps in creating and review of budgeting for cybersecurity.

The following are key steps in preparing a comprehensive cybersecurity budget as shown in Table 1.

Table 1: Key steps in creating and review of budgeting for cybersecurity.

Steps	Description
1) Get buy in from the top leadership	Alignment on budgeting from top leadership is critical to make sure that goals and allocations are realistic and can be carried out as envisioned.
2) Define your crown jewel and categorize key information assets	Identify and categorize key assets that need to be protected and identify the most sensitive data and critical infrastructure (i.e., "crown jewel") that requires a high level of effort to safeguard.
3) Assess your security posture	Determine security gaps and vulnerabilities in your current systems and determine the technical, human, and financial resources required.

4) Prioritize resource allocations	Assess asset vulnerability levels to prioritize cybersecurity budget allocation. Allocate more funds to crucial, high-risk assets, and allocate less to low-risk assets, as they have lower impact if a cyber breach were to occur.
5) Consider short term and long-term needs	Identify and address both short-term needs, like immediate software updates, and long-term goals, such as investments in advanced technologies and infrastructure needed to ensure readiness and preparedness for future cyber threat developments.
6) Allocate funds for incident response and recovery	Consider the likelihood of cyber incidents happening, its impact on the health system, and budget for the response and recovery from the cyber incidents.
7) Regularly review budget	Backed by a clear rationale, evidence, threat trends, and a deep understanding of organizational challenges, review the budget ensuring it aligns with regularly audited cybersecurity vulnerabilities and requirements to meet evolving security needs.

5.2 Key recommendations on developing and reviewing a cybersecurity budget.

Budgeting for cybersecurity should be aligned to the information security needs, tools and available resources as guided by checklists. Special considerations and measures should be made for activities that are to be carried out by or in collaboration with different ministries, to ensure effective and prompt execution. Once drafted, the budget should be validated with key stakeholders, and approved by top-level management.

Continuous monitoring is pivotal in ensuring security and privacy within health data systems. Insights gained from this ongoing process should drive adjustments in resource allocation and, if needed, prompt comprehensive budget reassessment. In cases of significant security breaches, urgent budgetary revisions might be essential, involving increased funding for specific areas and even the introduction of new budget lines.

Top leadership plays a determining role in influencing budgeting of cybersecurity. Notably, if there is no dedicated MoH budget for cybersecurity it is difficult for the MoH to contain the dynamic nature of cybersecurity and privacy. It is therefore recommended that MoH controls its own cybersecurity and privacy budget. It is further noted that countries that fail to formulate and review their budgets for their cybersecurity may end up having their cybersecurity security plans not aligned with the country's overall cybersecurity policies. Therefore, it is critical to get top leadership commitment as well as allocate adequate resources towards cybersecurity efforts.

There are three types of costs that require to be considered when budgeting for cybersecurity that include: Software and Hardware costs; Managed Services; and Training and Education. Detailed guidance on the development of an activity-based budget for cybersecurity is in Annex 3.

5.3 Budget template

A sample budget template is presented in Table 2.

Table 2: Budget template

Category	*Item*	*Source of Funds*	*Total amount allocated*	*Q1*	*Q2*	*Q3*	*Q4*	*Notes*
				Amount allocated	*Amount allocated*	*Amount allocated*	*Amount allocated*	
Software and hardware solutions	*Security System*							
	Antivirus tools							
	Intrusion Prevention/Detection Systems							
	Encryption software							
	Backup and recovery tools							
	Others							
Managed services	*Monitoring*							
	Maintenance							
	Updates							
	Audits							
	Cybersecurity insurance premiums							
	Others							
Training and Education	*Cyber training for employees*							
	Cyber training for other key stakeholders							
	Cyber education resources							
	Others							

5.4 Budgeting checklist

Table 3 provides a budgeting frameworks based on tools such as The Programming and Budgeting for Cybersecurity (58), the Stepwise Toolkit for Planning & Budgeting Interoperability of Digital Health Solutions by the Digital Health Centre of Excellence DICE (59)and the High level planning and budgeting guidance for sustainable District Health Information Software 2 DHIS2 (60) systems can be useful in meeting the below checklist.

The six dimensions used to organize this checklist are based on the NIST CSF (2). The *PROTECT* dimension is concerned with safeguarding health data systems by limiting any impact that may be caused by a cybersecurity incident. The *DETECT* dimension focuses on timely discovery of cybersecurity events and understanding their impact through continuous monitoring. The *RESPOND* dimension has to do with appropriate mitigation activities necessary when a cybersecurity incident has been detected to resolve it. The *RESTORE* or recover dimension deals with supporting timely restoration to normal operation following a cybersecurity incident, reviewing, and learning for purposes of future improvements. The *GOVERN* dimension brings in oversight, accountability, and alignment in the country's cybersecurity risk management.

Table 3: Budgeting checklist to ensure functional secure data systems.

Govern	Identify	Protect
• Does the budget address the necessary oversight activities as well as activities to review policies and procedures to support cybersecurity of health data systems? • Is the disbursement process robust enough to allow release of funds in good time for scheduled costs as well as for contingencies during incident response, even for activities between ministries? • Is the budgetary review process flexible enough to adapt to the dynamic threat landscape of cybersecurity and privacy?	• Is there an allocation to create an inventory and map of all the assets that need to be protected? • Is there an allocation to undertake an initial risk self-assessment as well as recurrent risk assessments? • Is there a budgetary allocation for the continuous monitoring of DHIs? • Is there an allocation to evaluate the effectiveness of continuous competency improvement of cybersecurity and privacy staff?	• Is there a budgetary allocation for purchase or leasing software and hardware controls for cybersecurity and privacy protection? • Is there an allocation for recurrent awareness training to all stakeholders including senior management, government officials, and the public? • Is there an allocation for specialized training for staff interacting with digital health data systems about cybersecurity and privacy threats? • Is there an allocation to keep all software and hardware up to date?
Detect	**Response**	**Restore**
• Is there an allocation for internal audit activities? • Are there funds allocated for threat detection tools such as antivirus, intrusion detection systems, malware, and ransomware detection systems? • Is there a budgetary allocation for the continuous monitoring of DHIs?	• Is there an allocation for recurrent training for key staff on disaster preparedness and response? • Are there funds for incident response software and hardware? • Is there an allocation for reporting and communicating on non-conformities? • Is there allocation for implementing contingency processes while responding to a cyber incident to ensure continuity of health services?	• Is there sufficient allocation of backups and restoration resources? • Where web-based health data systems are used, are there funds for mirrored services to ensure minimal downtime when disaster strikes? • Is there an allocation for regular activities to perform mock-up system restorations?

6. References

1. World Health Organization (WHO). Global strategy on digital health 2020-2025. Who [Internet]. 2021 [cited 2024 Feb 12];1–60. Available from: http://apps.who.int/bookorders.
2. NIST. The NIST Cybersecurity Framework 2.0 (Draft). 2023 Aug 8 [cited 2024 Feb 12]; Available from: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd
3. European Union. Regulation - 2016/679 - EN - gdpr - EUR-Lex [Internet]. [cited 2024 Feb 12]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
4. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Front Digit Heal. 2022 Aug 11;4:862221.
5. Shardul B. Legacy Systems Challenges in Healthcare and the Benefits of Migration [Internet]. 2023 [cited 2023 Nov 30]. Available from: https://www.tntra.io/blog/legacy-systems-challenges-in-healthcare/
6. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. J Med Internet Res [Internet]. 2021 Apr 1 [cited 2023 Nov 30];23(4). Available from: /pmc/articles/PMC8059789/
7. Point C. 2023 Mid-Year Cyber Security Report [Internet]. 2023 [cited 2024 Feb 12]. Available from: https://www.checkpoint.com/downloads/resources/2023-mid-year-cyber-security-report.pdf?mkt_tok=NzUwLURRSC01MjgAAAGOk6B-Pf-2dSK0S4YAnRiA_owAHrh8yQQqhSv8GGQJDfMQH3HHTg_uMBOJg2kw3oh-GJZdWmlA9PHfa-RVR9GxTPwoCv6sSXTqIBWzFIS2OWxVKZAy
8. Maggie Miller. The mounting death toll of hospital cyberattacks - POLITICO [Internet]. 2022 [cited 2024 Feb 12]. Available from: https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638
9. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare Data Breaches: Insights and Implications. Healthcare [Internet]. 2020 Jun 1 [cited 2022 Sep 12];8(2). Available from: /pmc/articles/PMC7349636/
10. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res [Internet]. 2018 May 1 [cited 2024 Feb 12];20(5). Available from: /pmc/articles/PMC5996174/
11. NCSA. National Cyber Security Authority | Official Website of NCSA [Internet]. [cited 2024 Feb 12]. Available from: https://cyber.gov.rw/home/
12. HHS. Summary of the HIPAA Privacy Rule | HHS.gov [Internet]. [cited 2024 Feb 12]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
13. WHO. Global Digital Health Certification Network [Internet]. [cited 2024 Feb 12]. Available from: https://www.who.int/initiatives/global-digital-health-certification-network
14. NIST. NIST Risk Management Framework | CSRC [Internet]. 2016 [cited 2024 Feb 12]. Available from: https://csrc.nist.gov/projects/risk-management/about-rmf
15. ISACA. About ISACA | A Global Business & Technology Community | ISACA [Internet]. [cited 2024 Feb 12]. Available from: https://www.isaca.org/about-us
16. ISO. ISO/IEC 27001 Information security management systems — Requirements [Internet]. [cited 2024 Feb 12]. Available from: https://www.iso.org/standard/27001
17. CMS. Federal Information Security Modernization Act (FISMA) - CMS Information Security & Privacy Group [Internet]. [cited 2024 Feb 12]. Available from: https://security.cms.gov/learn/federal-information-security-modernization-act-fisma
18. Ssc P. PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1 For merchants and other entities involved in payment card processing PCI

DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. 2009 [cited 2024 Feb 12]; Available from: www.pcisecuritystandards.org.
19. HSCC. Coordinated Healthcare Incident Response Plan (CHIRP).
20. OECD. OECD Recommendation on Health Data Governance - OECD [Internet]. [cited 2024 Feb 12]. Available from: https://www.oecd.org/els/health-systems/health-data-governance.htm
21. National eHealth Strategy Toolkit.
22. Force JT. Security and Privacy Controls for Information Systems and Organizations. 2020 Dec 10 [cited 2024 Feb 12]; Available from: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
23. ENISA. Introduction to Return on Security Investment — ENISA [Internet]. [cited 2024 Feb 12]. Available from: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
24. Petersen R, Santos D, Smith MC, Wetzel KA, Witte G. Workforce Framework for Cybersecurity (NICE Framework). 2020 Nov 16 [cited 2024 Feb 12]; Available from: https://csrc.nist.gov/pubs/sp/800/181/r1/final
25. ENISA. European Cybersecurity Skills Framework (ECSF) — ENISA [Internet]. [cited 2024 Feb 12]. Available from: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
26. ISACA. CMMI Institute - CMMI Levels of Capability and Performance [Internet]. [cited 2024 Feb 12]. Available from: https://cmmiinstitute.com/learning/appraisals/levels
27. Energy D of. Cybersecurity Capability Maturity Model (C2M2) | Department of Energy [Internet]. [cited 2024 Feb 12]. Available from: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
28. NRD CS. Cybersecurity Capacity Maturity Model for Nations (CMM) | NRD Cyber Security [Internet]. [cited 2024 Feb 12]. Available from: https://www.nrdcs.eu/cybersecurity-capacity-maturity-model-for-nations-cmm/
29. eGA. NCSI :: Methodology [Internet]. [cited 2024 Feb 12]. Available from: https://ncsi.ega.ee/methodology/
30. Blank RM, Gallagher PD. Guide for conducting risk assessments. 2012 [cited 2024 Feb 12]; Available from: http://csrc.nist.gov/publications.
31. Alberts CJ, Behrens SG, Pethia RD, Wilson WR. Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE SM) Framework, Version 1.0. 1999;
32. Authors V, Duhaney Richard B Harris Johanna G Vazzana Cynthia A Wright SY. Cyber Strategy Development & Implementation Framework Cyber Capacity Building. 2020;
33. ENISA. NCSS Good Practice Guide — ENISA [Internet]. [cited 2024 Feb 12]. Available from: https://www.enisa.europa.eu/publications/ncss-good-practice-guide
34. CIS. CIS Controls [Internet]. [cited 2024 Feb 12]. Available from: https://learn.cisecurity.org/cis-controls-download
35. OECD. Digital Security Risk Management for Economic and Social Prosperity. Digit Secur Risk Manag Econ Soc Prosper [Internet]. 2015 Oct 1 [cited 2024 Feb 12]; Available from: https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en
36. ISO. ISO 31000:2018 - Risk management — Guidelines [Internet]. [cited 2024 Feb 12]. Available from: https://www.iso.org/standard/65694.html
37. HSCC. Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO) - Health Sector Council [Internet]. [cited 2024 Feb 12]. Available from: https://healthsectorcouncil.org/hic-miso/
38. APEC. APEC Privacy Framework | APEC [Internet]. 2005 [cited 2024 Feb 12]. Available from: https://www.apec.org/publications/2005/12/apec-privacy-framework

39. ISO. ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines [Internet]. 2019. Available from: https://www.iso.org/standard/71670.html
40. Force JT. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. 2018 Dec 20 [cited 2024 Feb 12]; Available from: https://csrc.nist.gov/pubs/sp/800/37/r2/final
41. NCA. Home - National Cybersecurity Alliance [Internet]. [cited 2024 Feb 12]. Available from: https://staysafeonline.org/
42. ENISA. ENISA reports on cybersecurity investments, impact of NIS directive with deep dives into energy, health sectors - Industrial Cyber [Internet]. 2022 [cited 2024 Feb 12]. Available from: https://industrialcyber.co/reports/enisa-reports-on-cybersecurity-investments-impact-of-nis-directive-with-deep-dives-into-energy-health-sectors/
43. Unaids. The Privacy, Confidentiality and Security Assessment Tool: Protecting personal health information.
44. IMDRF. Final Document Principles and Practices for the Cybersecurity of Legacy Medical Devices AUTHORING GROUP Medical Device Cybersecurity Working Group. 2023;
45. HSCC. Medical Device and Health It. 2019;
46. HSCC. Managing Legacy Technology Security (HIC-MaLTS) Health Industry Cybersecurity. 2023;
47. UpGuard. Vendor Risk Assessment Template. 2022 [cited 2024 Feb 12]; Available from: www.upguard.com
48. ISO. IEC 81001-5-1:2021 - Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle [Internet]. 2021 [cited 2024 Feb 13]. Available from: https://www.iso.org/standard/76097.html
49. Chase M, Coley SC, Connolly J, Daldos R, Zuk M. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook [Internet]. 2022 [cited 2024 Feb 13]. Available from: https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response
50. UNAIDS. Interim Guidelines-1 GUIDELINES on PROTECTING the CONFIDENTIALITY and SECURITY of HIV INFORMATION: Proceedings from a Workshop.
51. Ježová D. PRINCIPLE OF PRIVACY BY DESIGN AND PRIVACY BY DEFAULT **. [cited 2024 Feb 13]; Available from: https://doi.org/10.18485/iup_rlr.2020.ch10
52. elev8. The Importance of Cyber Security Awareness Training [Internet]. 2023 [cited 2024 Feb 13]. Available from: https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees
53. ISO. ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls [Internet]. 2022 [cited 2024 Feb 13]. Available from: https://www.iso.org/standard/75652.html
54. Cichonski P, Millar T, Grance T, Scarfone K. Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology. 2012 [cited 2024 Feb 13]; Available from: http://dx.doi.org/10.6028/NIST.SP.800-61r2
55. Blank RM, Gallagher PD, Dempsey K, Shah N, Arnold C, Johnston JR, et al. Information Security Continuous Monitoring (ISCM) for federal information systems and organizations. 2011 [cited 2024 Feb 13]; Available from: http://csrc.nist.gov/publications.
56. Isaca. IT ASSURANCE FRAMEWORK (ITAF) FACT SHEET. [cited 2024 Feb 13]; Available from: www.isaca.org/itaf.
57. CIS. The Cost of Cyber Defense CIS Controls Implementation Group 1. 2023 [cited 2024 Feb 13]; Available from: https://www.cisecurity.org/controls/
58. Davis JS, Libicki MC, Johnson SE, Kumar J, Watson M, Karode A. A Framework for Programming

and Budgeting for Cybersecurity. 2016 [cited 2024 Feb 13]; Available from: www.rand.org/giving/contribute
59. DICE. Stepwise Toolkit for Planning & Budgeting Interoperability of Digital Health Solutions The DICE consortium. 2023;
60. DHIS2. Planning and Budgeting - DHIS2 Documentation [Internet]. 2023 [cited 2024 Feb 13]. Available from: https://docs.dhis2.org/en/implement/implementing-dhis2/planning-and-budgeting.html

7. Annexes

Annex 1: Types of costs and their justification for budgeting

Depending on cybersecurity maturity, mode of engagement with service providers, organization size, and key assets, cost categories will include cost drivers and specific budget line items as outlined below.

Cost categories	Activities	Description	Priority	Implication for not investing	Cost drivers
One-time costs to be incurred during deployment					
Training and education	Security planning	Cost of putting together a cybersecurity and privacy team composed of relevant stakeholders that will create and oversee a cybersecurity agenda that aligns with the country's goals and objectives. The team will determine the short term and long-term cybersecurity and privacy goals. The team will also draft the outline and prioritize the activities and budget for those activities	High	Lack of security and privacy planning may result in security plans that are not aligned with the country's overall policies. Also, insufficient budgeting may lead to plans that are not well prioritized to take the country to the highest maturity level	External expert staff, communication and travel, participant facilitation, data collection and analysis
Training and education	Cybersecurity and Privacy Maturity Self-Assessment	Costs incurred in establishing the level of maturity of the country as well as determining what needs to be done to eventually reach the highest level	High	Lack of awareness of the overall direction in which to focus cybersecurity and privacy efforts and countermeasures.	Maturity assessment software and hardware licenses and customization, external expert staff, communication and travel, data collection and analysis, participant facilitation
Managed services	Initial Risk Assessment	Costs incurred in identifying all relevant assets to patient-centric health data systems of the country as	High	Lack of an inventory of assets that need to be protected which may leave some assets unprotected. Lack of awareness	Risk assessment software and hardware license or purchase and

Cost categories	Activities	Description	Priority	Implication for not investing	Cost drivers
		well as performing a privacy risk assessment on the country's health data systems landscape to identify threats, vulnerabilities, and potential impact.		about which threats to focus effort in protecting to reduce the overall risk to the organization. Inability to approach privacy risk management in a structured, comprehensive manner	customization, external expert staff, communication and travel, data collection and analysis, participant facilitation
Software and Hardware solutions	Software and hardware security countermeasures setup	Costs associated with purchase or lease of intrusion detection systems, firewalls, antivirus, monitoring tools, etc. as well as their setup. The cybersecurity technologies solutions	High	Weak cybersecurity measures and high vulnerability. Information assets may be exposed to attackers. Also, it will take longer to detect that an incident has happened	Software and hardware license or purchase and customization, external expert staff, communication, and travel
Software and Hardware solutions	Local data center server setup or Local in-country private cloud setup	Costs associated with implementing a local server setup, or if possible, a local in-country private cloud service with a third party or a government owned data center	Medium	Some countries may see data being hosted outside of their country as a security risk	Server costs, data center costs, software and hardware license or purchase and customization, external expert staff, communication, and travel

Cost categories	Description	Priority	Implication for not investing	Cost drivers	Frequency
Recurrent costs					
Managed services	Costs incurred in regular risk assessments	High	Lack of adjustment of risk from the dynamic nature of the threat landscape may lead to unexpected impact. Misalignment and disharmony of real risks and risk mitigation efforts as cyber threat landscape and regulatory landscape increasingly mutate	Risk assessment software and hardware license or purchase and customization, external expert staff, communication and travel, data collection and analysis, participant facilitation	Half yearly
Personnel	Cost of skilled security staff who will operationalize the cybersecurity, privacy, and confidentiality plan. This could be a permanent staff with a monthly salary or a consultant dedicating several days in a week to the ministry	High	Exposure to increased vulnerability, limited incident response capabilities, inadequate security awareness, outdated policies, and an inability to keep pace with technological advances. The inability to attract and retain competent and skilled cybersecurity professionals further compounds these challenges. Skilled cybersecurity professionals are crucial for detecting and responding to threats, maintaining a security-aware culture, and ensuring compliance with evolving regulations.	Skill level and expertise, demand for talent, geographical location, industry, training and certification, retention and recruitment strategies, organization size and complexity, outsourcing, employee benefits, and turnover rates.	Monthly
Managed services	Cost of performing security assessment and privacy due diligence on vendors and partners that will work with the government on the health data systems. The assessment should check whether the vendor uses secure coding among other cybersecurity and privacy requisite practices	High	Possibility of onboarding partners that may increase your exposure and risk.	Risk assessment software and hardware license or purchase and customization, external expert staff, communication, and travel	Half yearly and during onboarding

Cost categories	Description	Priority	Implication for not investing	Cost drivers	Frequency
	concerning data handling.				
Managed services	Cost of Information Security Continuous Monitoring activities	High	Even with secure systems, lack of monitoring exposes systems to emerging attacks that have never been anticipated before. Also, attackers may exploit newly discovered bugs in the system	Continuous monitoring software such as SIEM tools, hardware license or purchase and customization, data storage, hosting and/or data center, external expert staff, hardware and software, communication and travel, data collection and analysis	Continuous
Training and education	Training costs of staff handling the health data systems as well as the users of those systems. Costs also include scheduled training on emerging technologies as well as how to deal with the dynamic threat landscape, including secure coding practices, disaster preparedness and response to key technical staff. For inhouse development teams, capacity building should include training on secure coding practices. Also included are regular awareness training to all staff on cybersecurity threats. Training on new privacy regulations and case law is also required	High	People are the biggest vulnerability. Lack of investing in local human capacity will increase the exposure of the health data systems. Skills deficiencies in emerging new cyberthreats and privacy requirements leading to unintended exposure. General users of the health data systems may fall prey to attackers through social engineering and other emerging people centered attacks. Knowledge deficiencies in emerging new cyberthreats	External expert staff, cybersecurity workshops, participant facilitation, online training and learning software license, hardware, communication, and travel	Quarterly and when necessary

Cost categories	Description	Priority	Implication for not investing	Cost drivers	Frequency
Software and hardware solutions	Recurrent costs associated with updates and or lease of intrusion detection systems, firewalls, antivirus, etc.	High	All software needs updating. Lack of investing in updates means that attackers can override control measures using new techniques that are not detectable by old software. This is especially relevant for Open-Source technologies or Global Goods with a limited developer to continuously patch the vulnerabilities.	Annual license for software and hardware countermeasure tools, external expert staff	Quarterly and when necessary
Managed services	Costs associated with maintaining a local data center with servers or a local in-country cloud service with a third party or a government owned data center	Medium	Some countries may see data being hosted outside of their country as a security risk	Data center costs, server costs, Cloud hosting costs, data center, external expert staff, annual software and hardware license, communication, and travel	Quarterly and when necessary
Managed services	Costs for continuous evaluation that actions taken are effective, including, including evaluating that the competency building of cybersecurity staff as well as feedback from citizens and stakeholders	High	Lack of investing in continuous evaluation will result in the country being unaware if the investment in cybersecurity is making the necessary impact.	External expert staff, key informant interviews, data collection and analysis, participant facilitation, communication and travel, evaluation software and hardware	Quarterly and when necessary
Managed services	Cost for performing internal and external audit to assess compliance with cybersecurity and privacy standards	High	Lack of investing in internal audits will result in lack of feedback on any non-conformance required cybersecurity and privacy requirements as well as to own country cybersecurity policies	External expert staff, audit hardware and software, participant facilitation, communication and travel, data collection and analysis	Half yearly
Managed services	Cost for placing relevant controls based on results from internal audit and risk assessment	High	Lack of treating risk may leave the digital health data systems vulnerable to exploitation	External expert staff, hardware and software purchase and customization, communication, and travel	When necessary

Cost categories	Description	Priority	Implication for not investing	Cost drivers	Frequency
Software and hardware solutions	Costs for performing mock restoration to practice and confirm effectiveness of backup and restoration	High	Not investing in activities for backup and restoration mocks may result in a false sense of security.	Participant facilitation, hardware and software, communication, and travel	Half yearly
Contingency					
Managed services	Costs associated with responding to incidents that may occur and costs associated with the process of recovering from those risks	High	Lack of investing or establishing a contingency plan in response and recovery means that when an attack happens, there is prolonged downtime, data may be lost or exposed.	External expert staff, hardware and software purchase and customization, communication and travel, data collection and analysis	On standby

Annex 2: Frequently asked questions

How do we get started with cybersecurity? Before investing in cybersecurity, it is crucial to assess a country's cybersecurity maturity level. The sections on creating and reviewing a budget for cybersecurity and key budget categories provide steps, guidelines, and considerations (one time and recurrent) for this. Additionally, it may be essential to identify the steps taken by countries with mature levels or standards in place and emulate their best practices.

How do we budget for cybersecurity and privacy? To have a comprehensive budget for cybersecurity and privacy, a country should consider having a checklist in place to guide the budgeting process. The contents of the checklist may vary depending on need but, they should capture the long- and short-term needs, digital assets to be budgeted for, sustainability of the budget, and change management. The section on budgeting checklist can aid in implementing a draft budget at all levels by the various stakeholders.

How do we implement cybersecurity, confidentiality, and privacy? There are several ways to ensure the implementation of cybersecurity, confidentiality, and privacy. Focus should be given to implementing strong security procedures such as encryption & proper key management, correct Identity & Access Management (IAM) configurations, right Access Control List (ACL) implementation (RBAC & ABAC), utilize hosted security agents in cloud, ingrain security practices from physical to application level, have a DLP procedure in place for onsite data and data hosted in the cloud, comply to given standards, and manage risks to information security as they arise, escalating cases to different levels for corrective actions.

How do we strengthen our cybersecurity and privacy posture? In order to improve a country's security **and privacy** posture, it is pertinent to perform Continuous monitoring and audits of systems, adherence to industry standards and guidelines, adherence to applicable regulations, performing patch management on systems, investing in human resources through training and awareness, having digital repositories for reporting of compliance statuses, in-placing contingent measures for backups and recoveries, implementing security and privacy by design principles in systems development, and budgeting to manage cybersecurity incidents.

Where can I learn about cybersecurity and privacy related topics? There are various resources on cybersecurity, however, for digital health implementation, one can focus on ISO 27799:2016 and ISO 27002 to get fundamental knowledge on areas of information security, and the focus on each. Additionally, given frameworks provide comprehensive guides such as NIST. For useful resources on privacy, see ISO 27701, country regulator websites such as the UK ICO, and the International Association of Privacy Professionals (IAPP).

How do I select a framework for cybersecurity and privacy? There exist several cybersecurity and privacy frameworks that can be implemented by different countries depending on need. For Digital Health, focus can be made to *ISO standards, CIS Controls, NIST, GDPR regulations, country regulations and industry standards.* Owing to its maturity and broad coverage, NIST is a perfect fit across multiple domains and covers comprehensively step by step from high level identification to low level recovery steps.

How do we plan for cybersecurity, and related incidences? The section on operationalizing secure data systems gives a step-by-step guide on how to plan, measures to have in place, stakeholders to engage, roles and responsibilities, proper budgeting with reference to checklists, risk assessments, risk treatments and risk mitigations.

What are the necessary measures when engaging vendors in health data systems? An assessment for the cybersecurity maturity level of the vendor is vital as well as an audit of the vendor's internal

security controls, as well as performing privacy due diligence on the vendors internal privacy controls.

Should we host our health data systems in-country or outside? It is preferred to host health data systems on a cloud regardless of whether it is a local cloud within the country or an external cloud provider. This is because of the benefits of cloud computing. A country may then decide, based on its cybersecurity maturity level, internal laws, regulations, policies, and guidelines, whether to use an in-country cloud or not.

Annex 3: Additional resources

Please note that some of the frameworks and standards may not be freely available, such as those from ISO.

- Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It. https://dsimg.ubm-us.net/envelope/136612/319602/1312920907_SANS_Continuous_Monitoring_WP.pdf
- Cyber Strategy Development and Implementation Framework (CSDI), MITRE Corporation. https://cybilportal.org/wp-content/uploads/2020/12/MITRE-CCI-CSDI-Framework-v4.0_2020_RELEASABLE.pdf
- Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs, CDC, https://www.cdc.gov/nchhstp/programintegration/docs/pcsidatasecurityguidelines.pdf
- Digital Security Risk Management for Economic and Social Prosperity https://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm
- Empowering a more secure, interconnected world, National Cybersecurity Alliance https://staysafeonline.org/
- Federal Information Security Management Act (FISMA) https://security.cms.gov/learn/federal-information-security-management-act-fisma
- Forrester's Targeted-Attack Hierarchy Of Needs, https://www.forrester.com/blogs/14-05-20-introducing_forresters_targeted_attack_hierarchy_of_needs/
- Global Digital Health Model Security Notice, GDHP https://gdhp.health/wp-content/uploads/2023/06/Proposed-Global-Digital-Health-MSN_CLEAN-Ver3_FINAL-DRAFT_06082023.pdf
- ISO 31000:2018 Risk management guidelines, ISO. https://www.iso.org/standard/65694.html
- National Capabilities Assessment Framework (NCAF), European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework
- National Cyber Security Index (NCSI), e-Governance Academy (eGA). https://ncsi.ega.ee/ncsi-index/
- National Cyber Security Strategy Good Practice Guide, European Union Agency for Network, and Information Security (ENISA). https://www.enisa.europa.eu/publications/ncss-good-practice-guide
- OECD Recommendation on Health Data Governance, https://www.oecd.org/health/health-systems/health-data-governance.htm
- Security and Privacy Controls for Information Systems and Organizations, NIST https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- Security Considerations for implementing DHIS2, https://docs.dhis2.org/en/implement/implementing-dhis2/security-considerations.html
- The Payment Card Industry Data Security Standard (PCI DSS) https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
- https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
- Building a Strong and Interoperable Digital Health Information System for Uganda, https://www.measureevaluation.org/resources/publications/fs-18-296/at_download/document
- Securing Digital Health, Initial reflections for steering global cyber security efforts in health, GDHP https://gdhp.health/wp-content/uploads/2022/11/Securing-Digital-Health-

Annex 4: Cybersecurity and privacy questionnaire

Guiding questions

a. Risk assessment

- What are the top cybersecurity and privacy concerns?
- What is the nature and number of cybersecurity and privacy threats?
- What are the key information assets?
- Which of your assets are most vulnerable to cybersecurity and privacy threats?
- How often is risk assessment and audits conducted on information assets?

b. Cybersecurity and privacy controls

- What are the existing cybersecurity and privacy controls?
- How often are cybersecurity risk assessments/analysis conducted?
- Are there measures in place for the detection, mitigation, and response to cyber security and privacy incidents?
- What is the adequacy of the existing cybersecurity and privacy controls?
    - Policies and strategies
    - Tools
    - Technologies
    - People

c. Cybersecurity budget and costs

- Has the cybersecurity budget changed in the last few years?
- What are the barriers to achieving a more realistic cybersecurity budget?
- What are the total costs spent in building cybersecurity and privacy controls every year?
- What are the annual monetary losses and costs associated with cybersecurity and privacy incidents?
- What are the annual non-monetary losses and costs associated with cybersecurity and privacy incidents?
- What are the effects of cybersecurity and privacy incidents?
- What is the total downtime (in hours) associated with cybersecurity and privacy incidents?
- Does insurance cover cybersecurity and privacy losses exist?

d. Policies and strategies

- Are the following policy documents available?
    - Cybersecurity Strategy
    - Cybersecurity policies
    - Cybersecurity procedures
    - Incident response plans, Business Continuity Disaster plans; and Disaster Recovery plans

e. Awareness and training

- Are there cybersecurity awareness programs offered?
- Does the top leadership board have sufficient understanding of the threats of digital technologies?