



Cybersecurity in Health

Digital technology, applications, data, and information systems, as part of the ongoing transformation of health and health care can help ensure universal and equitable access to affordable, people-centered, and integrated quality care, contributing to the goal of reaching Universal Health Coverage (UHC). Intelligent use of data and digital technologies can elevate patient experience, improve staff satisfaction, drive operational efficiency, improve patient outcomes, and create new business models, with benefits for both the public and private sectors.

This **Implementation Know-How Brief** provides World Bank Group **staff, country teams, and other organizations involved in the implementation of Digital-in-Health activities** with practical discussions, key terms and considerations, and broad guidance on how to engage with clients on the topic of **cybersecurity in health**.



This Brief Will Help Stakeholders to:

- Learn about **key cybersecurity terms and working definitions, the importance of cybersecurity in the health sector, and the most frequent types of cyber risks** in the sector
- Advise policy makers on **adopting an integrated approach to managing cyber risks** in the health sector through broad collaboration and public-private partnership
- Advise policy makers on the **elements and guiding principles of a cybersecurity strategy**, and its implications for the health sector
- Learn about **risk assessment methodologies to evaluate cyber risks, vulnerabilities, and threats** in the health sector
- Understand how to **manage cyber risks** through prevention, mitigation and recovery

Why Is Cybersecurity in Health Important?

As the health sector becomes increasingly reliant on digital technologies, it also becomes increasingly exposed to cyber risks, making cybersecurity in health a policy priority (the health sector includes all stakeholders involved in health, from patients, to health care providers, research institutes, insurance providers, pharmaceutical companies, information and communication technology providers, public health agencies, etc.). **Cyber incidents in health have far-reaching consequences.** A wide range of consequences arise from cyber incidents, affecting multiple parts of the health care sector. These repercussions involve both direct and

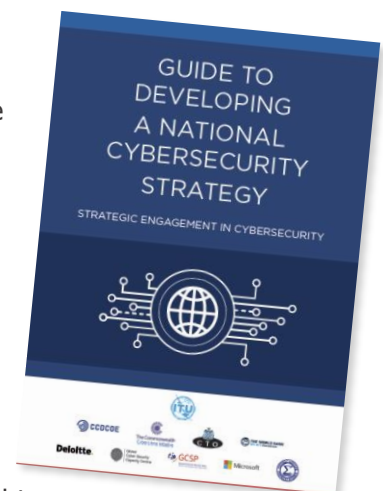
indirect impacts. They encompass negative outcomes such as delays in patient care, heightened risks to patient safety resulting in higher rates of mortality and morbidity, compromised quality of care due to limited access to health information, increased stress and anxiety among staff members involved in incident response, reduced confidence in the security of personal health data, and a broader erosion of trust in the healthcare sector's ability to effectively and efficiently handle cyber risks and deliver high-quality care (CyberPeace Institute 2021)¹.

The number and severity of cyber incidents in health are on the rise. In a 2021 survey of hospital executives in the United States, 48 percent reported either a forced or proactive shutdown in the six months prior to the survey due to external attacks or queries, with large hospitals reporting an average shutdown time of 6.2 hours at the cost of US\$21,500 per hour and midsize hospitals averaging nearly 10 hours at US\$45,700 per hour (Ipsos 2021). In a survey of 5,600 information technology professionals across 31 countries, 66 percent of health care organizations reported being hit by ransomware in 2021, a 94 percent increase from 2020². The average cost to remediate an attack was US\$1.85 million, and 25 percent of health care organizations that suffered an attack took up to a month to recover. According to IBM, the cost of a data breach in the health care industry has gone up 42 percent since 2020, and for the 12th year in a row, the health sector had the highest average data breach cost of any industry, at US\$10.10 million³. In 2017, hospitals in 150 countries, including Japan, China, Indonesia, and Taiwan, were hit by the global ransomware attack WannaCry (Marsh & McLennan Companies 2018). According to data from health care organizations in 43 countries (including Australia, Brazil, Thailand, Colombia, India, and Jordan), over 500 organizations have been targeted, more than 21 million records breached; systems went offline in 52 percent of incidents; data were leaked or exposed in 69 percent of incidents; ambulances or patients were diverted in 13 percent of incidents; appointments or surgeries were canceled in 16 percent of incidents; and operational disruption ranged from a few hours to 115 days⁴. Africa is not immune to cyber incidents in the health sector. In 2017, in African countries, like Nigeria, South Africa, and Kenya, hospitals were affected by the global WannaCry ransomware attack. The attack disrupted health care services and compromised patient data.

What is Cybersecurity?

There are many definitions for the term *cybersecurity* (or *cyber security*; these two terms are typically used interchangeably). To avoid misunderstandings, Task Teams should be aware that different countries and organizations use different definitions.

The **working definition used in this brief** is that of the International Telecommunication Union (ITU) "Guide to Developing a National Cybersecurity Strategy", co-developed with the World Bank (Council of Europe (CoE), et al. 2021): "the term *cybersecurity* is meant to describe the collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance, and technologies that can be used to



protect the availability, integrity, and confidentiality of assets in the connected infrastructures pertaining to government, private organizations, and citizens; these assets include connected computing devices, personnel, infrastructure, applications, digital services, telecommunications systems, and data in the digital-environment". Cybersecurity is a broad topic, touching on many different aspects including governance, policy, operations, technologies, and legislation.

While this brief focuses on *cybersecurity*, it may be helpful for Task Teams working in health to learn about the Organization for Economic Co-operation and Development (OECD) Policy Framework on Digital Security, which defines *digital security* as a set of measures taken to manage digital security risk for economic and social prosperity (OECD 2022a). For the OECD, *cybersecurity* relates to the security of technical assets (for example, health information systems and networks; see definition from ITU above) while *digital security* refers to the security of the economic and social activities that rely on those technical assets (for example, delivery of emergency health services). To illustrate, a cyberattack on a health care facility may subvert both the security of technical assets (for example, by causing the facility to shut down its information technology systems) and the security of economic and social activities (for example, by causing the facility to divert urgent care to other facilities).

Key Cybersecurity Terms and Language

Cybersecurity seeks to manage cyber risks, through prevention and mitigation (OECD 2022a)⁵. Cyber risks are a function of the likelihood that a cyber incident occurs, and the potential impact or severity resulting from that cyber incident. *Cyber incidents* are events that disrupt the availability, integrity and/or confidentiality (AIC or CIA triad; see ITU's definition above) of technical assets (for example, data, software, hardware, and networks). By rendering technical assets inaccessible or unusable (availability), altering assets without authorization (integrity), and giving access to assets to unauthorized entities (confidentiality), cyber incidents negatively affect the activities that rely on these assets.

Cyber incidents are caused by intentional/adversarial or unintentional/accidental threats that exploit vulnerabilities. Intentional threats are often called cyberattacks while unintentional threats include human errors, natural disasters, or system failures. Threats are characterized by actors (sources of threats, for example, hackers), and tools and techniques (threat vectors, for example, malware). Malicious actors can range from unskilled individuals with limited resources to well-resourced State-sponsored actors pursuing geopolitical goals. *Vulnerabilities* are weaknesses in people (for example, training and awareness), processes (for example, backup procedures or systematic vulnerability management) and technologies (for example, software code).


Finally, certain assets and activities are so crucial for the health, safety, and security of citizens, and for the effective functioning of services essential to the economy, society, and the government, that they are considered critical and require a higher level of protection. **Critical Infrastructures are assets that are essential to the functioning and security of a society and economy in any given nation, and Critical Information Infrastructures**

are information and communication technology systems that operate key functions of the critical infrastructure of a nation (Council of Europe (CoE), et al. 2021). *Critical activities*, also called critical functions of essential services, are activities that depend on critical infrastructures (Bernat 2021).


Cybersecurity Risks and Threats in the Health Sector


As the health sector increasingly embeds digital technologies, it becomes exposed to cyber risks. This is particularly true during periods of crisis (such as the COVID-19 pandemic and military conflict), when the health system is especially vulnerable to intentional and unintentional threats (Price et al. 2022; CISA 2021). **Factors behind health systems' vulnerability to cyber incidents include** (ENISA 2021b; CyberPeace Institute 2021):


-  **Health care is a critical activity**, crucial to the proper functioning of societies and economies. Due to health care providers' increasing reliance on information and communication technologies, it is difficult to implement technical solutions without disrupting the continuous delivery of health care services. The critical nature of health care services with potentially grave implications in terms of morbidity and mortality, and the need to keep services running 24/7/365 also makes health care providers targets for cyberattacks.
-  **Health data are a valuable target** for malicious actors due to their sensitive nature and market value. Health records contain personal data: information that relates to an identified or identifiable living individual. Moreover, personal data concerning health is considered to merit the highest standards of protection in European and American data regulations.
-  **Health care systems often depend on legacy systems** that were designed a long time ago and are vulnerable to modern-day cyberattacks. Replacing these systems is not without challenge, and modular solutions may add complexity by increasing the number of interconnected systems (and actors). Coupled with the growing adoption of medical and Internet of Things (IoT) devices, the attack surface is expanding (attack surface is the sum of digital security vulnerabilities). Furthermore, to overcome what they consider technological barriers to quality patient care, health care professionals may circumvent security measures, thus further increasing digital security vulnerabilities.
-  **Health systems are hugely complex**, with many sub-systems and stakeholders. This complexity is reflected in incident response, involving a potentially large number of individuals with possibly unclear roles and responsibilities dealing with a cascade of negative effects.
-  There is **limited exchange of information and best practices in cybersecurity in health** at both national and international levels.


 **Health systems lack expertise and specialists** in both information technology generally and cybersecurity specifically. This lack of human capacity manifests itself in ineffective prevention and incident response. While awareness of cyber risks among frontline health workers is increasing, **health care professionals do not always have the tools and know-how** to adequately manage digital security risks. There is **limited investment in cybersecurity in health**, and smaller health care providers and industry players frequently have limited financial capacity to adopt cybersecurity practices.

According to the European Union Agency for Cybersecurity (ENISA), **technical assets in health care that can be vulnerable to cyber risks** include (ENISA 2019):


 **Remote care system assets**, including medical equipment for remote monitoring and diagnosis such as heart rate monitors, glucose meters, and drug dispensers.


 **Networked medical devices**, such as implantable or wearable devices like insulin pumps, cardiac pacemakers, stationary devices like magnetic resonance imaging or X-ray equipment.


 **Identification systems** to authenticate and track patients, staff and equipment, such as radio frequency identification (RFID) tags and systems, bracelets, and smart badges.

 **Networking equipment** used in health care establishments, such as network devices (routers, switches), cables, wireless equipment, and computers.


Mobile client devices, like laptops, smartphones, tablets, and applications working on them.


 **Interconnected clinical information systems** including, among many others, Laboratory Information Systems, Radiology Information Systems, Blood Bank Systems


 **Data** including administrative patient data, clinical data (for example, health records, test results, medical history), and research data (for example, clinical trials results).



 **Physical infrastructure in health** such as buildings, electricity supply, air conditioning.

Cyber risks and threats in health can be categorized into (according to ENISA's taxonomy; categories may not be mutually exclusive, although it is helpful to think in terms of root cause, for example, in phishing the root cause is a malicious action even though human error may play into it):

 **Malicious actions**, including malware (for example, viruses, worms, trojans, rootkits), hijacking, denial of service (DoS) attacks, device tampering, social engineering (for example, phishing), theft of device, theft of data, and skimming (credit/debit card information theft).

 **Human errors**, due to involuntary human actions, resulting in digital security incidents.

 **System failures**, including software or firmware failures, device failure, network failure, insufficient maintenance, and overloading.

-  **Supply chain failure**, caused by inadequate risk management from, for example, cloud providers, network providers, power supply providers or manufacturers of medical devices.
-  **Natural phenomena**, including fires, floods, earthquakes, and other natural disasters that can affect technical assets and cause interruption of normal services.

Steps and Measures to Improve Cybersecurity in Health

Due to the critical nature of health care for societies and economies, the ubiquity of cyber risks and vulnerabilities in the health sector, the potentially catastrophic consequences for patients and the already high and rising direct and indirect costs of cybersecurity incidents in health, taking measures to improve cybersecurity in health is imperative, and an essential step towards a successful digital transformation in health that delivers benefits for all. Task Teams should take note of the following basic premises when thinking through cybersecurity in the context of health:

- **Cybersecurity is often to some extent centralized.** The Ministry of Health, and subnational health authorities, may not have mandates to take measures to improve cybersecurity in the health sector. Collaboration with the national or subnational mandated agency or agencies for cybersecurity is crucial for promoting a cybersecurity agenda in health. It is paramount that World Bank health sector financing that includes the digitalization of health sector data or the use of digital technologies, consider the extent to which, and ways in which, cybersecurity is addressed in the government and in the health sector, and seek to understand health sector-specific weaknesses that can be addressed through World Bank operations.
- **Cybersecurity is a responsibility shared by all stakeholders.** While the Ministry of Health, and subnational health authorities, may legislate, regulate, and promote cybersecurity practices in the health sector, it is patients, health workers, providers, and industrial organizations (to name a few of the stakeholders/operators involved) that ultimately take cyber risks depending on their risk tolerance. The implications for government involvement are clear: as health care is a critical activity for societies/economies, operators cannot be the sole decision makers. While there is guidance directed at operators, there is much less for policy makers.
- **Cybersecurity risks are dynamic and can never be eliminated**, unless the social and economic activity that depends on digital assets ceases to exist. Cyber risks can be reduced through cybersecurity risk management, but there is always some residual risk that will have to be taken. This is why recovery and resilience are key to improving cybersecurity.
- **Cybersecurity is not an end in and of itself**, but rather a means to protect health care activities, from delivering care to disease surveillance and pharmaceutical research and development, to name a few. Measures taken to protect health care activities that rely on digital assets need to support these activities in achieving their

objectives and need to be proportional to the risks. Proportionality is key, because cybersecurity measures can also inhibit the activities that they are trying to protect by increasing costs, reducing performance, and altering the open and dynamic nature of the digital environment.

Different countries, regions, and organizations are starting from very different maturity levels both in terms of digital health maturity as well as minimum cybersecurity standards. Although there are no international assessments of cybersecurity in health, the most recent edition (2020) of the all-sectors Global Cybersecurity Index found very significant differences in cybersecurity measures across its 193 Member States and the State of Palestine (International Telecommunication Union 2020). According to the World Bank⁶, only 20 percent of African states currently have the basic legal frameworks in place for countering cybercrime, and since 2020 there is an estimated shortage of 100,000 proficient cybersecurity personnel. Kenya is one example of an African country investing in cybersecurity (Republic of Kenya 2022). Given the broad heterogeneity in digital health maturity and cybersecurity practices across countries, there is no standardized approach to cybersecurity in health that would be effective in all contexts. Task Teams should work with clients to design customized programs that fit their clients' needs.

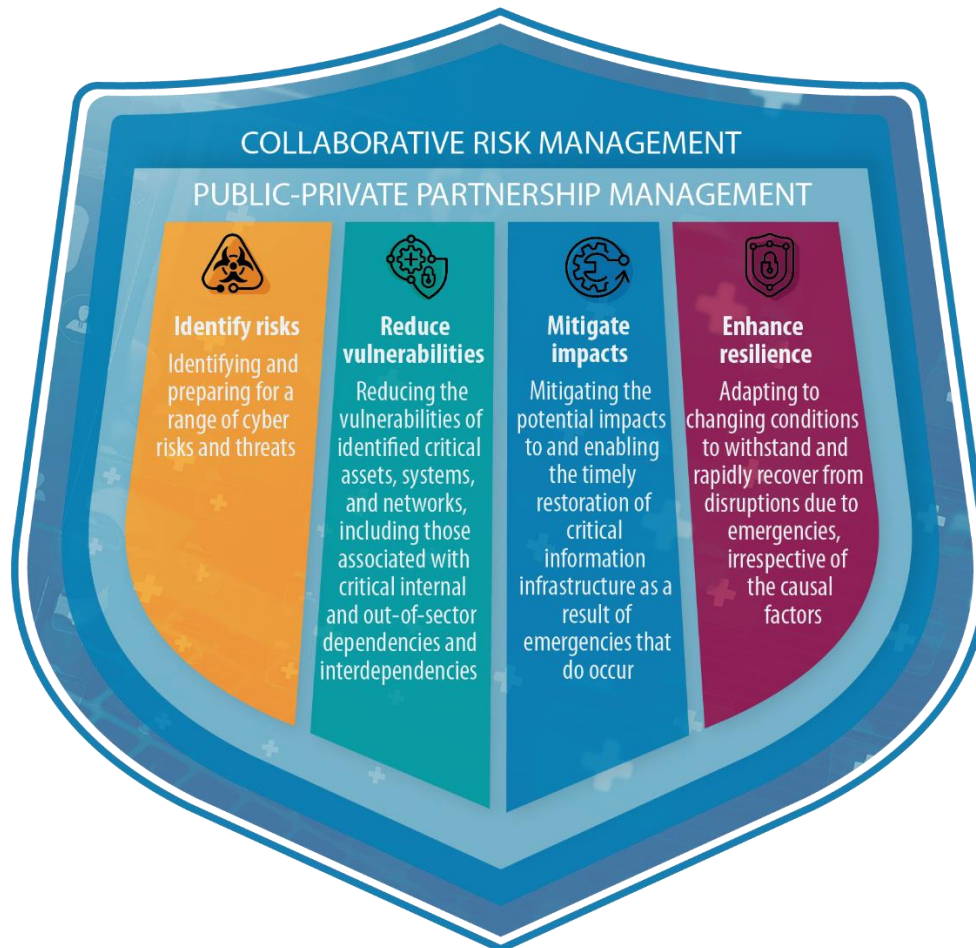
Finally, as with all digital health initiatives, the implementation of cybersecurity measures and practices in health should be well-aligned with the Principles for Digital Development⁷, specifically: designing with the user; designing for scale; being data driven; using open standards, open data, open source, and open innovation; addressing privacy and security; and being collaborative.

Key Considerations for Policy Makers in Health

It is challenging to identify key considerations and implementation steps for government authorities seeking to improve cybersecurity in health because **there is very limited guidance designed specifically for policy makers in the health sector**. Existing maturity models, toolkits, and frameworks tend to focus either on cybersecurity practices across all sectors (for example, the Cybersecurity Capacity Maturity Model for Nations) or on cybersecurity practices at organizational level (for example, the United States NIST Cybersecurity Framework). There are two exceptions that focus on cybersecurity in health at organizational level: the Essentials of Cybersecurity for Healthcare Organizations or ECHO framework and the Health Care and Public Health Sector Cybersecurity Framework Implementation Guide (O'Brien et al. 2020; U.S. Department of Health and Human Services 2023). Examples of maturity models and frameworks are provided in annex.

This brief focuses on describing the **key elements that are vital at national level for policy makers seeking to improve cybersecurity in health**. Concrete steps will differ from country to country, and context to context, but the overall approach illustrated in figure 1 holds at national level.

Figure 1 Integrated approach to managing cyber risks in the health sector



Source: Based on U.S. Department of Homeland Security and U.S. Department of Health and Human Services 2016.

Based on the United States Department of Homeland Security's "Healthcare and Public Health Sector-Specific Plan", the integrated approach illustrated above rests on the public and private health sectors coming together to evaluate risks, coordinate plans and policy, and provide guidance on the five key functions of cybersecurity: prevention, protection, mitigation, response, and recovery. From the perspective of the Ministry of Health, this means bringing together many stakeholders to share information. Table 1 illustrates the goals and near-term priorities of an integrated approach to improving cybersecurity in health.

Table 1 Goals and near-term priorities of health sector integrated approach to cybersecurity






Goals		Near-term priorities
Risk assessment 	Leverage relationships and resources to assess and analyze threats to, vulnerabilities of, and consequences of disruption to health sector critical information infrastructure to inform risk management activities. Ensure that approaches consider elements of critical information infrastructure security and resilience, supply chain issues, and interdependencies with other sectors	<ul style="list-style-type: none"> Plan and execute a risk assessment methodology to assess the cyber risks, vulnerabilities, and threats in the health sector
Risk management 	Enhance the resilience of the health sector by translating risk analyses into actionable recommendations for operators (for example, public health departments, public and private sector facilities, industry). Integrate such risk analyses into the mitigation, response, and recovery efforts of the central government. Execute risk mitigation activities in a prioritized manner with clear plans and metrics for success	<ul style="list-style-type: none"> Develop a long-term risk mitigation plan and set priorities based on a health sector risk assessment, leveraging existing products developed by partners, health care trend analyses, and needs of critical information infrastructure owners and operators Develop guidance for health sector implementation of a cybersecurity framework
Information sharing 	Enhance existing and develop new mechanisms to ensure bidirectional sharing of information. Promote sharing of risk information, threats, best practices, and lessons learned between government and private sector partners	<ul style="list-style-type: none"> Assess the effectiveness of current processes, mechanisms, and systems used to share information among health sector partners Strengthen the dialogue between government and private sector partners about the challenges and benefits of two-way information sharing, particularly with respect to what can be shared, and cybersecurity incidents and gaps
Partnership development and coordination 	Develop and implement a “Partnership Engagement Strategy” to include outreach efforts to both government and private sector entities with a focus on developing relationships with owners and operators of critical information infrastructure. Encourage development of partnerships across geographies and sectors to enhance health sector resilience, facilitate information sharing, and respond to incidents	<ul style="list-style-type: none"> Develop a “Partnership Engagement Strategy” that enhances existing and develops new outreach material and determines key partners that are not currently engaged cybersecurity activities Analyze and broaden partnerships to support critical information infrastructure security and resilience and to better understand the relationship between health sector critical information infrastructure and community resilience.

Table continued...

Table 1 Goals and near-term priorities of health sector integrated approach to cybersecurity (continued)

Goals		Near-term priorities
Response and recovery 	Engage in response and recovery efforts across government agencies, health care coalitions, and the private sector during and after cybersecurity incidents. Exercise the ability of the health sector to respond to adversarial and accidental cyber incidents and incorporate lessons learned into future exercises and corrective actions	<ul style="list-style-type: none"> ▪ Clarify health sector response and recovery roles and functions among government, health care coalitions, and the private sector ▪ Exercise the entire health sector partnership at the sector level and through national-level cybersecurity exercises

Source: Based on U.S. Department of Homeland Security and U.S. Department of Health and Human Services 2016.

Naturally, the integrated approach to improving cybersecurity in health must be coordinated and well aligned with efforts to promote cybersecurity at the national level across all sectors. One such effort that may be in place is a **National Cybersecurity Strategy**. The International Telecommunications Union, the World Bank, the OECD, the African Union, the European Union, all these organizations have either promoted or even mandated (in the case of the European Union and its 2016 Network and Information Security Directive) that Member States adopt national cybersecurity strategies. These strategies contain the vision, high-level objectives, principles, and priorities that guide a country in addressing cybersecurity; provide an overview of the stakeholders tasked with improving cybersecurity of the nation and their respective roles and responsibilities; and give a description of the steps, programs, and initiatives that a country will undertake to protect its national cyber infrastructure and, in the process, increase its security and resilience (Council of Europe (CoE), et al. 2021). Having a national cybersecurity strategy, and/or a sectoral cybersecurity strategy, can be instrumental in raising basic awareness of cybersecurity.

The “Guide to Developing a National Cybersecurity Strategy” identifies **good practice examples across seven focus areas or themes** (the order is not supposed to imply relative importance), from which countries can take inspiration based on their own objectives and priorities (Council of Europe (CoE), et al. 2021). While not specific to the health sector, all or most of the good practice examples can be applied to a strategy for improving cybersecurity in the health sector.

Table 2 National cybersecurity strategy focus areas and good practice examples

Focus area: Governance

- Ensure the highest level of support
- Establish a competent cybersecurity authority
- Ensure intra-governmental cooperation
- Ensure inter-sectoral cooperation
- Allocate dedicated budget and resources
- Develop an implementation plan

Table continued...

Table 2 National cybersecurity strategy focus areas and good practice examples (continued)**Focus area: Risk management in national cybersecurity**

- Conduct a cyber threat assessment and align policies with the ever-expanding cyber threat landscape
- Develop sectoral cybersecurity risk profiles
- Establish cybersecurity policies

Focus area: Preparedness and resilience

- Establish cyber-incident response capabilities
- Establish contingency plans for cybersecurity crisis management and disaster recovery
- Promote information-sharing
- Conduct cybersecurity exercises
- Establish impact or severity assessment of cybersecurity incidents

Focus area: Critical Infrastructure and essential services

- Establish a risk-management approach to identifying and protecting critical infrastructure and essential services
- Adopt a governance model with clear responsibilities
- Define minimum cybersecurity baselines
- Utilize a wide range of market levers
- Establish public private partnerships

Focus area: Capability and capacity building and awareness raising

- Strategically plan capability and capacity building and awareness raising
- Develop cybersecurity curricula
- Stimulate capacity development and workforce training
- Implement a coordinated cybersecurity awareness raising program
- Foster cybersecurity innovation and research and development
- Tailor programs for vulnerable sectors and groups

Focus area: Legislation and regulation

- Establish a domestic legal framework for cybersecurity
- Establish a domestic legal framework on cybercrime and electronic evidence
- Recognize and safeguard human rights and liberties
- Create compliance mechanisms
- Promote capacity-building for law enforcement
- Establish inter-organizational processes
- Support international cooperation to combat cyber threats and cybercrime

Table continued...

Table 2 National cybersecurity strategy focus areas and good practice examples (continued)**Focus area: International cooperation**

- Recognize cybersecurity as a component of foreign policy and align domestic and international efforts
- Engage in international discussions and commit to implementation
- Promote formal and informal cooperation in cyberspace
- Promote capacity building for international cooperation

Source: (Council of Europe (CoE), et al. 2021).

Note: See also OECD 2022b; For Governance specifically, see also (ENISA 2023). 07/08/2023 09:21:00

Assessing Cybersecurity Maturity and Cyber Risks

The first element of the integrated approach is an **assessment of cybersecurity risks and capabilities in the health sector**. The near-term priority is to plan and execute a risk assessment methodology to assess cyber risks, vulnerabilities, and threats in the health sector, both at national/subnational level and at operator level. Table 3 illustrates the range of approaches to cybersecurity risks assessments (many maturity models and frameworks are also provided in annex). Task Teams should seek and review previous assessments (even if from all-sector cybersecurity maturity models) to fill gaps and achieve efficiencies (to avoid conducting unnecessary duplicative assessments).

Table 3 Categories/types of digital and cybersecurity risk assessments

Risk assessment scope and focus areas	<ul style="list-style-type: none"> ▪ Organizational information and communication technology systems approach⁸. ▪ Sectoral-level approach⁹ ▪ National-level approach¹⁰ ▪ Regional-level approach¹¹
Basic approaches at national level	<ul style="list-style-type: none"> ▪ The centralized risk assessment (or state-driven approach) is a one-size-fits-all model, in which the coordinating authority requires identified actors (health care operators) to implement a particular or unified standard for risk assessments. For example, the United Kingdom has implemented this risk management approach ▪ In the decentralized risk assessment (or operator-driven approach), each identified actor (health care operator) prepares its own risk assessment to be integrated by a coordinating authority. For example, Sweden, Denmark, Japan, and Switzerland have implemented decentralized risk assessment approaches

Table continued...

Table 3 Categories/types of digital and cybersecurity risk assessments (continued)**Methodologies**

- In the scenario-based approach, identified actors are gathered to consider scenarios in the round; the scenarios describe risks as a narrative and label them by applying simple categories of likelihood and impact (low, medium, high). For example, the telecommunication sector in Denmark has used this risk assessment approach
- In the qualitative approach, countries with a specific threat modelling technique in place tend to use qualitative models; qualitative assessments are the usual approach used by countries when deciding upon the significance of a threat. Qualitative models with a broad range of threats are common in Nordic countries
- The quantitative approach applies ordinal thresholds (for example, specific risks are classified as severe if they affect 200 in 20,000 or outages for five days or more). For example, Japan has implemented this approach
- The hybrid approach combines all the above elements (for example, using scenarios and then qualitative and quantitative methods). For example, the Netherlands has implemented this model

Source: World Bank 2021.

At the national level, the World Bank Digital Government Readiness Assessment Toolkit suggests that assessments of cybersecurity should include the following questions (World Bank 2020):

- Has the government developed a cybersecurity strategy and policy document?
- Has the government established a cybersecurity unit or center within a core entity to manage and maintain security of all digital assets and platforms? If yes, are there government entity cybersecurity functions established and staffed?
- Is there a Computer Incident Response Team (CIRT) capability in the government? Does the government collaborate with regional and international governments or organizations to share information on and mitigate cyber threats or risks?
- Does the government have a National Critical Infrastructure Protection Plan? If yes, does it include digital government infrastructures, platforms, and services?

The World Bank is committed to providing funding and technical assistance to client countries to strengthen their national cybersecurity capacities, for example by implementing the Cybersecurity Capacity Maturity Model (the World Bank has done this in multiple countries). The World Bank also deploys multiple development projects worldwide to strengthen the cyber resilience of critical infrastructures in the information and communication technology and financial sectors.

At a broader level, beyond cyber risks, it could be useful to assess the status of cybersecurity practices in health using the WHO/ITU building blocks for electronic/digital health (see table 4). A consideration of these building blocks can help temper expectations of what policy makers seeking to improve cybersecurity in health can achieve when there are fundamental barriers. Low-income countries typically have poor infrastructure (lack of stable electricity, unreliable

Internet connectivity, inadequate computer equipment), limited technical support, low computer skills and training, mixed record systems (for example, electronic and paper), and insufficient funding (Ngugi et al. 2021; Ferry et al. 2021; Odekunle, Odekunle, and Shankar 2017; Akhlaq et al. 2016). A push for cybersecurity practices in health should take these challenges into account, for example by making parallel investments in information infrastructure.

Table 4 Digital health building blocks: non-exhaustive list of considerations

Legislation, policy, and compliance

- Are there laws, regulations, or guidelines concerning cybersecurity?
- Is there a national cybersecurity strategy? Does the strategy reference health specifically?

Leadership and governance

- Is there a national or sectoral cybersecurity authority?
- Are national or sectoral Computer Incident Response Teams (CIRTs) in place?
- Is there cross-border cooperation on cybersecurity (in general and in health)?

Interoperability and standards

- Are there international standards and technical guidelines on cybersecurity in use in health?
- Is there a body dedicated to supervising compliance of regulated entities with standards/guideline?
- Is there a cybersecurity certification scheme that applies to health in place?

Workforce

- Is there awareness of cyber risks and appropriate training and skills development in cybersecurity in health?
- Do health organizations have designated employees to coordinate and be accountable for cybersecurity?

Strategy and investment

- Are there sufficient financial resources for all health organizations to implement cybersecurity practices?
- Given enabling environment and existing infrastructure, how could cybersecurity practices affect health inequities?
- Are there well-funded mechanisms for monitoring the effective use of cybersecurity practices in health?

Infrastructure; Services and applications

- Is there an inventory of technical assets in health and their vulnerabilities? Are there legacy systems?
- Have elements of the critical information infrastructure been identified?

Source: Based on World Health Organization and Union 2012; ENISA 2023.

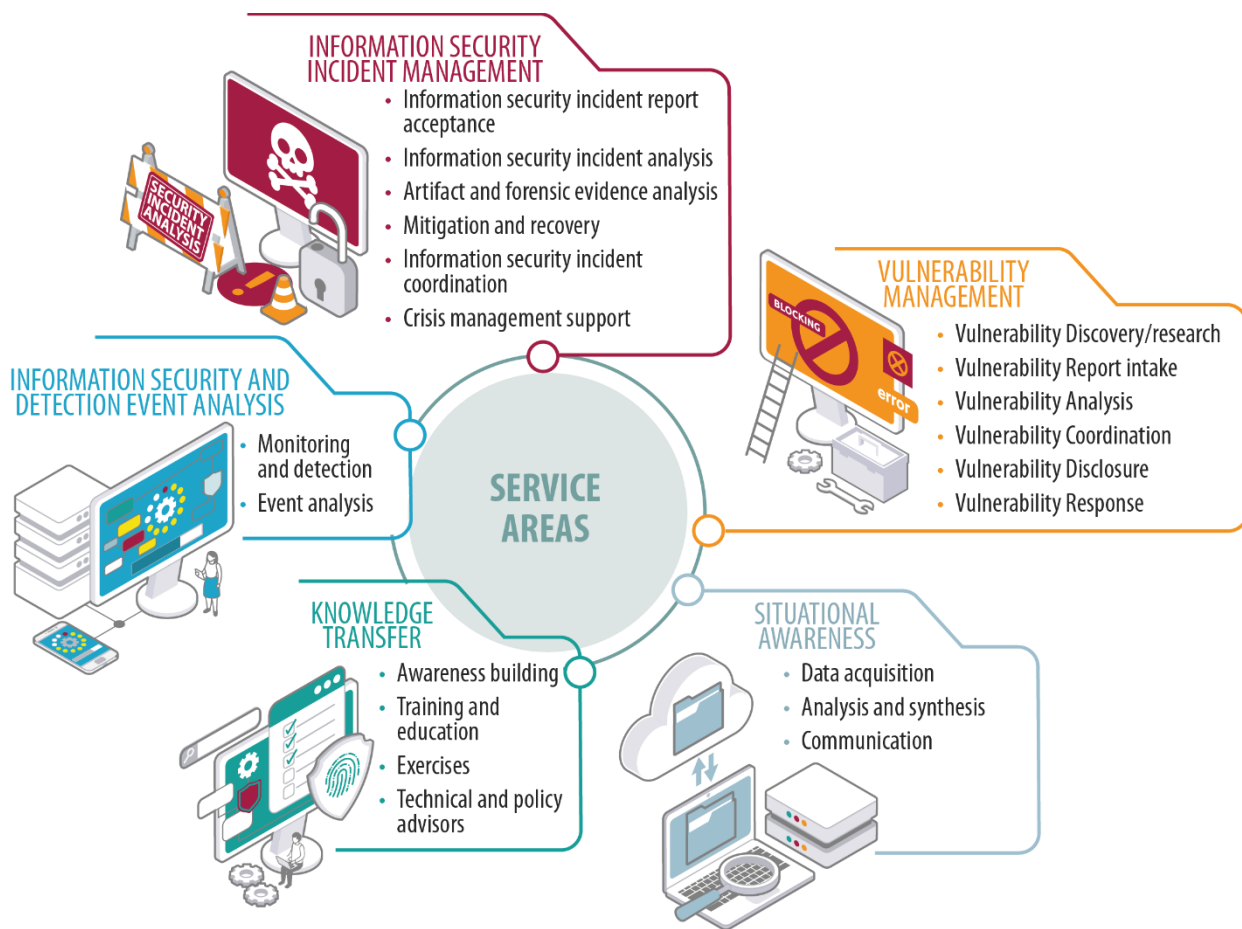
Note: There is some overlap between categories (for example, workforce issues are also often legislation and policy issues).

Managing Cyber Risks: Prevention, Mitigation and Recovery

After assessing cybersecurity risks and capabilities, as well as overall digital maturity and readiness for cybersecurity, the priorities are to reduce vulnerabilities and prevent cyber threats, to develop a long-term risk mitigation plan and set priorities, and to provide guidance for health sector implementation of a cybersecurity framework.

Prevention of cybersecurity threats involves the implementation of cybersecurity measures and solutions designed to reduce vulnerabilities of identified critical assets, systems, and networks, including those associated with critical internal and out-of-sector dependencies and interdependencies. Estimated resources needed for the prevention of cyberattacks will vary depending on the country context and level of cyber maturity. Prevention measures can target humans (for example, through training and raising awareness), technologies (for example, by implementing firewall protection and vulnerability audits), and processes (for example, via strong credential and password policies). Strong leadership is crucial to implement prevention measures.

Task Teams may find that at the national level there will already exist so-called Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs) or Computer Incident Response Teams (CIRTs). Whatever the specific term used, **these teams are typically responsible for responding and coordinating responses to cyber incidents**; managing cyber vulnerabilities; raising awareness of cyber risks/threats and providing education; and situational awareness (see figure 2). National CIRTs also play a crucial role in international coordination and collaboration (ENISA 2022)¹². CIRTs can be set up at various levels (for example, national, regional, sectoral, organizational). The European agency ENISA has recommended that countries “enhance and facilitate the creation of health sectoral CSIRTs” (ENISA 2021b)¹³

Figure 2 CSIRT services framework service areas and services

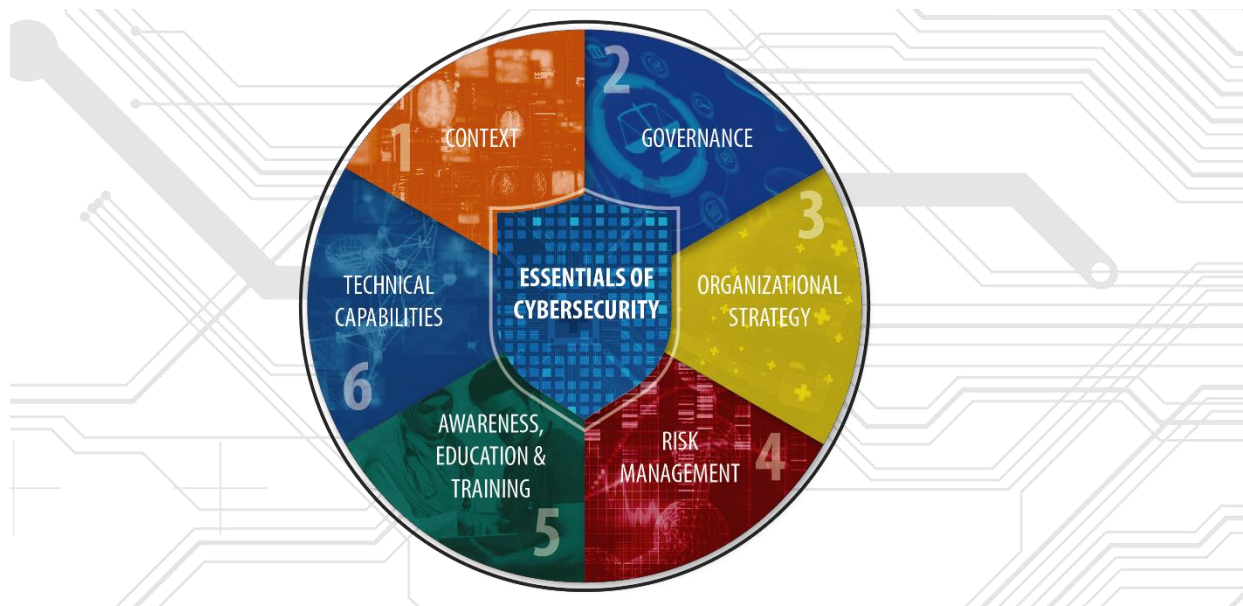
Source: FIRST.org 2019.

All the service areas shown above are important, but two—**knowledge transfer and vulnerability management**—are especially relevant in the context of health given current maturity levels and cyber risks previously discussed. Cybersecurity is a shared responsibility. Everyone, from policy makers to health care professionals, health managers, medical device producers, the information and communication technology industry, to patients and communities, everyone has a part to play in maximizing cybersecurity. It is **important that all stakeholders are aware of cyber risks** and that they feel that they can report vulnerabilities and share information.

Policy makers should also **develop guidance for health sector implementation of a cybersecurity framework at organizational level**. An organizational cybersecurity framework provides a common language and structure for discussions of cyber risks and ways to manage cyber risks to levels that are acceptable to the organization but also other stakeholders, from investors to clients and government (U.S. Department of Health and Human Services 2023). There are two health sector specific cybersecurity frameworks at organizational level: the Essentials of Cybersecurity for Healthcare Organizations or ECHO framework and the Health Care and Public Health Sector Cybersecurity Framework Implementation Guide (O'Brien

et al. 2020; U.S. Department of Health and Human Services 2023). The ECHO framework contains six primary dimensions to consider when scaling up cybersecurity in a health care organization (see figure 3), and may act as a 'minimum standard' or an aspirational checklist. The Health Care and Public Health Sector Cybersecurity Framework is based on the United States National Institute for Standards and Technology (NIST) framework. The framework's five high-level functions are to Identify, Protect, Detect, Respond, and Recover (see figure 4 for an illustrative example of a scorecard). Whatever cybersecurity framework is adopted by any individual organization, it is crucial that policy makers promote the adoption of frameworks among health care organizations.

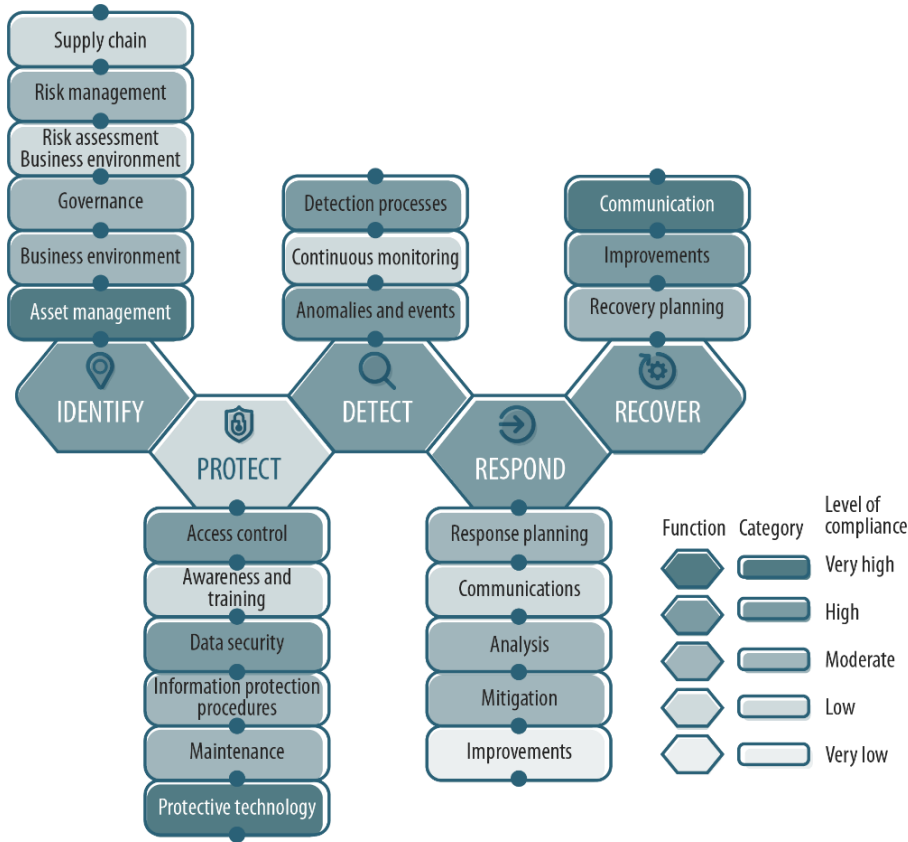
Figure 3 Essentials of cybersecurity for healthcare organizations (ECHO) framework



Source: O'Brien et al. 2020.

Because risks can never be eliminated, **cyber insurance is a way for health care organizations to manage their exposure**, protect their assets, clients, employees, and balance sheet. Moreover, cyber insurance can help organizations show that they are taking cyber risks seriously and complying with best practices. Indeed, the European Union Agency for Network and Information Security has found a positive correlation between cyber insurance take-up and the level of cybersecurity preparedness (Marsh & McLennan Companies 2018). Among the requirements that underwriters could look for in organizations seeking to acquire cyber insurance are email filtering, patch and vulnerability management, protection for end-of-life systems, awareness training, cyber incident response testing, and vendor supply chain management¹⁴.

Figure 4 Illustration of a NIST cybersecurity framework scorecard



Source: U.S. Department of Health and Human Services 2023.

Finally, the Royal Australian College of General Practitioners has developed **a compliance checklist designed to assist general practices and other office-based health care organizations** to meet their professional and legal obligations in computer and information security (Table 5). The full document provides detailed guidance on achieving different levels of maturity for each standard (The Royal Australian College of General Practitioners 2013).

Table 5 Compliance checklist for computer and information security in general practice

Roles and responsibilities

- Do you have designated practice team members for championing and managing computer and information security and do these practice team members have such roles and responsibilities documented in their position descriptions?** This will include a written policy that is communicated to practice team members, the assignment and training of a Computer Security Coordinator, the assignment and training of the Responsible Officer and Organization Maintenance Officer, and the national eHealth record system training where applicable.

Table continued...

Table 5 Compliance checklist for computer and information security in general practice (continued)**Risk assessment**

- ❑ **Have you undertaken a structured risk assessment of information security and identified improvements as required?** This will include recording assets in the practice, a threat analysis, reporting schedule and data breach recording procedures.

Information security policies and procedures

- ❑ **Do you have documented policies and procedures for managing computer and information security?** This will include a policy to cover each Standard. It will also include practice team and external service provider agreements, and where applicable an eHealth records system policy

Managing access

- ❑ **Do you have well-established and monitored authorized access to health information?** This will include a clearly defined and communicated policy that contains direction on access rights, password maintenance, password management, remote access controls, and auditing and appropriate software configuration.

Business continuity and information recovery

- ❑ **Do you have documented and tested plans for business continuity and information recovery?** This will include tested, practical and implementable business continuity and information recovery plans to ensure business continuation and prompt restoration of clinical and business information systems

Internet and email usage

- ❑ **Do you have processes in place to ensure the safe and proper use of internet and email in accordance with practice policies and procedures for managing information security?** This will include details of configuration and usage of the internet and email, together with practice team education in good internet and email use practices.

Information backup

- ❑ **Do you have a reliable information backup system to support timely access to business and clinical information?** This will include documented procedures for the systems to be backed up and how often (backup type and frequency, use of encryption, reliability and restoration checking, media type and rotation, where the backup is stored and who has access to it). It should also include access to data from any previous practice information (legacy) systems.

Malware, viruses and email threats

- ❑ **Do you have reliable protection against malware and viruses?** This will include automatic updating of the virus protection software and educating the practice team to be aware of risks of exposing the practice information systems to malware and virus attack.

Table continued...

Table 5 Compliance checklist for computer and information security in general practice (continued)**Computer network perimeter controls**

- ❑ **Do you have reliable computer network perimeter controls?** This will include ensuring the firewall is correctly configured and that the log files are examined periodically; this will also apply to intrusion detection systems. Wireless networks need to be appropriately configured, and content filtering and perimeter testing should be considered.

Mobile electronic devices

- ❑ **Do you have processes in place to ensure the safe and proper use of mobile electronic devices in accordance with practice policies and procedures for managing information security?** This will include the defined use and secure management of practice-owned and personal mobile devices that are used for business or clinical purposes.

Physical facilities and computer hardware, software and operating system

- ❑ **Do you manage and maintain the physical facilities and computer hardware, software and operating system with a view to protecting information security?** This will include the physical protection of equipment and the use of an uninterruptible power supply (UPS). A secure disposal process should be established and appropriate system and software maintenance undertaken.

Security and information sharing

- ❑ **Do you have reliable systems for the secure electronic sharing of confidential information?** This will include the appropriate configuration of secure messaging, digital certificate management and the practice website.

Source: The Royal Australian College of General Practitioners 2013.

Other specific cases that may merit special attention in the health sector include **digital and cybersecurity in hospitals and digital and cybersecurity in the cloud** (ENISA 2020; 2021a). The European agency ENISA has published guides on these two topics. One provides hospital procurement officers and chief information security officers (or chief information officers) with a comprehensive set of tools and good practices that can be adapted to the hospitals' procurement process to ensure that cybersecurity objectives are met. The other guide provides cloud security practices for the health care sector and identifies security aspects, including relevant data protection aspects, to be considered when procuring cloud services for the health care industry.

The Ministry of Health and other stakeholders (for example, professional associations) can provide guidance to health care organizations, for example using compliance checklists like the one shown above, but also through **setting and disseminating standards, whether optional or mandatory**. Security standards have been developed by countries (for example, United States NIST) and international organizations (for example, ISO). The latter has developed several widely used security standards, such as ISO/IEC 27032 (guidelines for cybersecurity), ISO/IEC 27001 (information security management systems), ISO 22301 (business continuity management systems), ISO/IEC 15408 (evaluation criteria for IT

security), ISO/IEC 27035 (information security incident management), and ISO/IEC 27005 (information security risk management) (World Bank 2021). Certain standards focus on specific sectors, such as ETSI GR IP6 008 V1.1.1 (2017-06), which is focused on IPv6-based IoT deployment.

The World Bank has highlighted an existing patchwork of cybersecurity certification schemes and initiatives worldwide, with different countries recognizing different schemes (or none; see footnote for link). The European agency ENISA (ENISA 2019), building on previous security recommendations for IoT and medical devices, has identified **common high level functional security requirements for health products and services, to be evaluated during the certification process** (see table 6).

Table 6 ENISA’s cybersecurity requirements for health products and services

Security by design

- Consider the security of the whole system from a consistent and holistic approach [P, O]*
- Ensure the ability to integrate different security policies, technologies, and methods [P, O]
- Consider risk posed to human safety; carry out a risk assessment in relation to the specific application area [P, O]
- Design for power conservation should not compromise security [P]
- Design architecture by compartments to encapsulate elements in case of attacks [P]
- Test plans to verify whether the product or service performs as it is expected (like penetration tests) [P, O]
- Code review during implementation to reduce bugs [P]

Personal data protection / privacy by design

- Make personal data protection and privacy an integral part of the design of a system or product or service [P, O]
- Perform personal data protection / privacy impact assessments [P, O]
- Establish and maintain asset management procedures and configuration controls [P, O]
- Identify significant risks using a defense-in-depth approach [P, O]
- Identify the intended use and environment of a given device [P]
- Follow a layered approach recognizing the importance of treatment of health care data as sensitive personal data, which calls for different measures than those taken for other general types of data [O]

Table continued...

Table 6 ENISA's cybersecurity requirements for health products and services (continued)**Organizational measures**

- Put in place and implement an effective security policy [P, O]
- Carry out a security risk assessment regularly [P, O]
- Ensure appropriate business continuity and disaster recovery plans [P, O]
- Establish a secure development life cycle [P]
- Develop a full end-of-life strategy [P]
- Offer effective and secure patch management [P]
- Use proven solutions, well known communications protocols and cryptographic algorithms [P, O]
- Establish procedures for security incident handling [P, O]
- Participate in information sharing and coordinated vulnerability disclosure [P]
- Ensure the personnel is trained in privacy and security [P, O]
- Cybersecurity roles and responsibilities are established [P, O]
- Develop policy for processing of data by a third-party [P, O]
- Adopt cyber supply chain risk management policies [P, O]
- Make broad use of recognized solutions to known issues, even when it is not mandated by legislation [P]

Technical measures

- Meet baseline security requirements for IoT [P]
- Carry out a risk assessment regarding the specific application area and complete it with suitable mitigation measures [O]
- The use of recognized solutions to known issues, even when it is not mandated by legislation, for the management of administrative data is desirable, as health care systems require a high level of assurance [P, O]
- Ensure appropriate configuration of information and communication technology systems and their segregation [P, O]
- Deploy cybersecurity measures to protect data at rest, in use and in motion [P, O]
- Apply appropriate traffic filtering [O]
- Use state-of-the-art cryptography and key storage methods [P, O]
- Put in place effective identity and access management [P, O]
- Ensure correct information technology security maintenance [P, O]
- Develop policies for physical and environmental security [P, O]
- Deploy early warning/detection systems [P, O]

Source: Based on ENISA 2019 (see Annex 1 of citation for baseline security requirements for IoT).

Note: * = O denotes operators of services; [P] = requirements for manufacturers of products.

Information Sharing and Partnership Development

Working with the centralized national agency, or agencies, for cybersecurity, the Ministry of Health should **promote the sharing of risk information**, threats, best practices, and lessons learned between government and private sector partners; as well as **encourage the development of partnerships** across stakeholders, geographies, and sectors to enhance health sector resilience, facilitate information sharing, and respond to incidents. As the government entity ultimately responsible for health care, the Ministry of Health is best placed to coordinate the sector's stakeholders. Concentrating responsibilities for information sharing and partnership development and coordination under one organization—be it a sectoral health CIRT, a national agency for cybersecurity in health, or an existing digital health agency—could be appropriate.

Final Considerations

Improving cybersecurity in the health sector is likely to require significant financial and human resources, and for countries with limited cybersecurity maturity in health, the development, promotion, and dissemination of good cybersecurity practices in health will probably be long and complex, involve many stakeholders and require much of their time, and likely require very close collaboration across different sectors. In lower resource contexts, it is plausible that major investments in basic building blocks (for example, supply of electricity and broadband connectivity, information infrastructure, and capacity building) will be needed in parallel with efforts to improve cybersecurity. New laws, regulations, guidelines, and institutions may be needed, as well as professionals with the required skills in the country.

It is important to consider that many health care organizations—especially smaller ones like single private practices—may not have the resources to implement comprehensive cybersecurity practices. Financial incentives to promote implementation should be included in government budgets for cybersecurity in the health sector. If appropriate, incentives should be tied to performance metrics to ensure good value for money (for example, use of certified technologies). Governments, for their part, should lead by example, including by adopting best practices and by using public procurement to foster risk management in the sector (OECD 2022a).

Task Team Leaders may be interested to learn about **the World Bank's Cybersecurity Multi-Donor Trust Fund**¹⁵, which was developed as an associated trust fund under the broader Digital Development Partnership Umbrella (DDP) and aims to better define, understand, articulate, structure, and roll-out the cybersecurity development agenda in a systematic manner. The emerging work program offers comprehensive cybersecurity capacity development, including development of global knowledge, country assessments, technical assistance, capacity building and training, underpinned with necessary investments in infrastructure and technology.

Finally, efforts to improve cybersecurity in health do not end, rather this is a journey of continuous improvement and optimization. **Cybersecurity risks, vulnerabilities, and threats,**

as well as the economic and social activities that rely on digital technologies, these are all dynamic. Monitoring, evaluation, and learning are crucial to ensuring that practices are (still) achieving their intended goals, are comprehensive, and are not leading to unintended consequences (for example, stifling innovation and digital transformation). A first step in this process is determining what success looks like, how it will be measured, and what are the key indicators that need to be collected, potentially for the first time ever. Monitoring and evaluation should then lead to continuous learning and improvement. The maturity assessment frameworks listed in annex are naturally good references for what indicators to monitor.

Key Challenges and Pitfalls

Cybersecurity in health is still developing, even in high-income countries with more advanced levels of digital health maturity (as evidenced by growing number and severity of cyber incidents). The Ministry of Health does not necessarily have the leadership in cybersecurity in the sector, and it is likely that coordination at national level with other sectors will be needed. Moreover, there is a lack of guidance on this topic developed specifically for the health sector. For all this, Task Teams should be mindful that solutions will be country and context specific. Furthermore, Task Teams should seek a good balance between promoting good cybersecurity practices in the context of their specific projects (for example, implementation of a digital health record system in primary health care, development of a national system for managing health insurance claims, etc.) and promoting a more holistic integrated approach to cybersecurity in health, as described in this brief. Regardless, there are several challenges and key pitfalls to be aware of (examples shown in table 7).

Table 7 Examples of challenges in improving cybersecurity in health

As a shared responsibility across so many stakeholders, with so many different systems, there are **significant coordination challenges and difficulties aligning all players** around digital and cybersecurity.

Forgetting the **human element of cybersecurity** and focusing mostly on the technology/infrastructure.

Limited resources for cybersecurity strategy implementation may lead to unfunded mandates.

Not conducting a cyber risk assessment at the appropriate levels (for example, national, organizational).

Limited incentives for information sharing and vulnerability disclosure. Disincentives for security researchers (“white hats”, “friendly hackers”) to find and disclose vulnerabilities, including the use of punitive measures.

Cybersecurity risk management should not hinder digital transformation and innovation. **Cybersecurity should not be an end in and of itself** but a means to promote the use of digital technologies for economic and social objectives.

Poor cybersecurity governance can lead to chaotic and ineffective responses to cyber incidents.

Source: Expanded from OECD 2022c.

Other Resources

African Union Convention on Cybersecurity and Personal Data Protection:

<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection/>

ENISA's Sets of Key Performance Indicators on Cybersecurity, in Annex B, page 61 of:

<https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies>

ENISA's List of tools in service for the five service areas of CSIRTs, on Table 5, page 24 of:

<https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector>

ENISA's Baseline Security Recommendations for IoT: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

ENISA's Network and Information System Investments 2022:

<https://www.enisa.europa.eu/publications/nis-investments-2022>

ENISA's Procurement Guidelines for Cybersecurity in Hospitals:

<https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>

European Union Medical Device Coordination Group (MDCG) Guidance on Cybersecurity for medical devices: <https://ec.europa.eu/docsroom/documents/41863>

The OECD Global Forum on Digital Security for Prosperity: <https://www.oecd.org/digital/global-forum-digital-security/>

Cyber Incident Tracer #HEALTH: <https://cit.cyberpeaceinstitute.org/>

Cyber Europe 2022: After Action Report: <https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report>

National Cybersecurity Index: <https://ncsi.ega.ee/>

Singapore's Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure:

https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf?sfvrsn=a63bf6d8_0

IDB Observatory of Cybersecurity in LAC, including country profiles: <https://cybersecurityobservatory.org>

ITU Cybersecurity Index: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

Council of Europe's Octopus Cybercrime Community Country Wiki:

<https://www.coe.int/en/web/octopus/country-wiki>

United Nations Institute for Disarmament Research Cyber Policy Portal: <https://cyberpolicyportal.org/>

World Bank CyberTalks: Cyber Resilience Event Series:

<https://www.worldbank.org/en/events/2022/11/15/digital-development-cybersecurity-event-series>

CyberPeace Institute's Cyber 4 Healthcare: <https://cyberpeaceinstitute.org/cyber4healthcare/>

MITRE's Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook and Quick Start Companion Guide: <https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response>

OECD's Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities: [https://one.oecd.org/document/DSTI/CDEP/SDE\(2021\)9/FINAL/en/pdf](https://one.oecd.org/document/DSTI/CDEP/SDE(2021)9/FINAL/en/pdf)

National Cybersecurity Strategies:

European Union Agency for Cybersecurity's National Cybersecurity Strategies Interactive Map: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

Canada's National Cybersecurity Strategy: <https://www.publicsafety.gc.ca/cnt/rsracs/pblctns/ntnl-cbr-scr-strtg/index-en.aspx>

United States Department of Health and Human Services Knowledge on Demand cybersecurity education platform: <https://405d.hhs.gov/knowledgeondemand>

United States Department of Health and Human Services cybersecurity resource library (including how-to guides): <https://405d.hhs.gov/resources>

United States Department of Health and Human Services Cybersecurity Practices for Small Healthcare Organizations: <https://405d.hhs.gov/Documents/tech-vol1-508.pdf>

United States Department of Health and Human Services Cybersecurity Practices for Medium and Large Healthcare Organizations: <https://405d.hhs.gov/Documents/tech-vol2-508.pdf>

United States Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) Recommended Cybersecurity Practices: <https://healthsectorcouncil.org/hsc-cc-publications/>

USAID's Cybersecurity Primer: https://www.usaid.gov/sites/default/files/2022-05/10-26-21_EXTERNAL_CyberPrimer-CLEARED-accessible.pdf

Overview of OECD Council Recommendations on Digital Security: https://www.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en

Relevant World Bank Case Studies



Improving Cybersecurity in Health Checklist

This checklist is for national and subnational levels; it can be printed as a stand-alone document.

Adopting an integrated approach to managing cyber risks

- Bring together the public and private health sectors to evaluate** risks, share information, coordinate plans and policy
- Provide guidance on the five key functions of cybersecurity:** prevention, protection, mitigation, response, and recovery

Assessing cybersecurity maturity and cyber risks

- Plan and execute a risk assessment methodology** to assess the cyber risks, vulnerabilities, and threats in the health sector
- Assess the status of cybersecurity practices** in health using the WHO/ITU building blocks for electronic/digital health (including the enabling environment: Leadership and Governance; Strategy and Investment; Legislation, Policy and Compliance; Workforce; and Standards and Interoperability; and the information and communication technology environment: Infrastructure; and Services and Applications)

Managing cyber risks: prevention, mitigation and recovery

- Reduce vulnerabilities** and prevent cyber threats
- Develop a **long-term risk mitigation plan** and set priorities
- Identify CIRT** at national level. Consider creation of sectoral health CIRT
- Provide **guidance for health sector implementation** of a cybersecurity framework
- Consider the use of **cyber insurance for health care organizations** to manage their exposure, protect their assets, clients, employees, and balance sheet
- Consider the use of **compliance checklists and best practice guides** for specific health care subsectors (for example, general practice, procurement in hospitals, cloud services)
- Promote **good practices** through standards setting

Information sharing and partnership development

- Consider **concentrating responsibilities** for information sharing and partnership development and coordination under one organization—be it a sectoral health CIRT, a national agency for cybersecurity in health, or an existing digital health agency
- Identify **indicators for assessing performance and impact**, and for evaluating success
- Plan for **continuous improvement and optimization**
- Adopting an **integrated approach to managing** cyber risks
- Bring together the public and private health sectors** to evaluate risks, share information, coordinate plans and policy

Acknowledgements

This implementation know-how brief was written by Tiago Cravo Oliveira Hashiguchi, Malarvizhi Veerappan, and Marelize Görgens. It benefited greatly from comments and feedback from Giacomo Assenza, Anat Lewin, Boris Volkov, Charles William Dalton, Hermann Pythagore Pierre Donfouet, and Niki O'Brien. The brief was edited by Harriet Stella Blest and graphically designed by Theo Hawkins. The development of the implementation know-how brief series was prepared under the supervision of Malarvizhi Veerappan and Marelize Görgens.

Background on Implementation Know-How Briefs

What is an Implementation Know-How Brief and What is it For?

The World Bank's Digital-in-Health: Unlocking the Value for Everyone report calls for a new digital-in-health approach where digital technology and data are infused into every aspect of health systems management and health service delivery for better patient outcomes. The report proposes ten recommendations across three priority areas for governments to invest in: prioritize, connect and scale. The Implementation Know-How Briefs serve as practical, implementable extensions to the Digital Health Flagship report. The Implementation Know-How Briefs take a practical approach to discussing a topic with the aim of describing the topic, the key terms and technical considerations, guidance on how to start an operational engagement with clients on the topic, relevant checklists (if applicable), links and places to go for help.

The aim of Implementation Know-How Briefs is to give Task Teams enough information to figure out how a given topic fits into Health, Nutrition and Population (HNP) investments, and what are the right questions to ask. The aim is not to make Task Teams topic experts. The Implementation Know-How Briefs also tackle the dependencies between different topics.

Who is this Implementation Know-How Brief For?

The Implementation Know-How Briefs are focused on World Bank Task Teams, countries, and other organizations involved in implementation of Digital-in-Health activities and extend the discussion on the topics covered in the Digital Health Flagship report.





Who is Responsible for Implementation Know-How Briefs?

Digital Health Flagship Research Program: digitalinhealth@worldbank.org.



Annex 1





Theory of Change

Cybersecurity in health theory of change			
 Gaps in Cybersecurity in Health	 Cybersecurity in Health	 Outcomes	 Impact
<ul style="list-style-type: none"> Health care is a critical activity that is especially vulnerable to digital and cybersecurity risks, particularly during a crisis The health sector is reliant on complex, vulnerable, under-resourced, and outdated digital assets. Cybersecurity vulnerabilities and risks are poorly managed Consequences of cybersecurity incidents in health can be catastrophic Costs of cybersecurity incidents in health are substantial 	<ul style="list-style-type: none"> Adopt an integrated approach to improving cybersecurity in health grounded on collaboration and private-public partnership Plan and execute an assessment methodology of cyber risks, vulnerabilities, and threats Develop a long-term risk mitigation plan and set priorities based on risk assessment Develop guidance for health sector implementation of a cybersecurity framework Promote information sharing and partnership development and coordination 	<p>Shorter- and medium-term</p> <ul style="list-style-type: none"> Cybersecurity helps health sector achieve objectives without undue burden Increased trust and confidence in the digital health environment Effective, safe, and responsive health care Increased investments and donor funding Strengthened collaboration between client countries <p>Longer-term</p> <ul style="list-style-type: none"> Higher levels of maturity for cybersecurity in health 	<ul style="list-style-type: none"> Universal and equitable access to affordable, people-centered, and integrated quality care Good governance of health systems for sustainable financing and accountability for health outcomes Augmented service delivery value chain Reinvigorated essential public health functions

Examples of Maturity Models, Toolkits and Frameworks

There are multiple sets of maturity models, assessment tools, and frameworks available, but it is important to note that they are not specific to health (see the table A1). Moreover, not all tools are for macro assessments (for example, the C2M2 maturity model is for organizations). Task Team Leaders advising clients on digital and cybersecurity in health could consider exploring one or more of these documents, after reading this implementation know-how brief, remembering that each document's insights need to be translated to both the national and the health contexts.

Table A1 Examples of digital and cybersecurity assessment tools and frameworks

Examples of digital and cybersecurity assessment tools	
Resource	Overview, focus and purpose
<p>Essentials of Cybersecurity in Healthcare Organizations Institute of Global Health Innovation (IGHI) at Imperial College London and Leading Health Systems Network, 2020</p> <p>Link here</p> 	<p>The ECHO framework is based on components identified by a panel of global experts as the most important elements of a global cybersecurity framework for healthcare. It outlines the six primary dimensions to consider when scaling up cybersecurity in a healthcare organization. The framework offers a common language for the essential issues that need to be addressed. It may be viewed as a 'minimum guide' or an aspirational checklist, depending on an organization's cyber maturity and resources.</p> <p>Geographies: Global</p> <p> BEST FOR: cybersecurity framework specifically designed for health</p>
<p>Cybersecurity Capacity Maturity Model for Nations (CMM) Global Cybersecurity Capacity Centre (GSCC) at Oxford University, last updated in 2021</p> <p>Link here</p> 	<p>The Cybersecurity Capacity Maturity Model for Nations (CMM) is a methodical framework designed to review a country's cybersecurity capacity. The CMM considers cybersecurity to comprise five dimensions which, together, constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity: 1) developing cybersecurity policy and strategy; 2) encouraging responsible cybersecurity culture within society; 3) building cybersecurity knowledge and capabilities; 4) creating effective legal and regulatory frameworks; and 5) controlling risks through standards and technologies. The CMM defines five Stages of maturity for all dimensions being: start-up, formative, established, strategic, and dynamic.</p> <p>Geographies: Global</p> <p> BEST FOR: national assessments of cybersecurity capacity</p>

Continued on next page...

Examples of digital and cybersecurity assessment tools (continued)

Resource

Global Cybersecurity Index Framework | ITU, last updated in 2020

[Link here](#)



Overview, focus and purpose

The ITU framework for international multi-stakeholder cooperation in cybersecurity aims to build synergies between current and future initiatives and focuses on five pillars, which shape the inherent building blocks of a national cybersecurity culture: legal measures; technical measures; organizational measures; capacity building measures; and cooperative measures. There is a total of 20 indicators across the five pillars, with scores constructed from 82 questions.

Geographies: Global

BEST FOR: national assessments of cybersecurity capacity

National Cybersecurity Index (NCSI) | e-Governance Academy Foundation, last updated in 2023

[Link here](#)



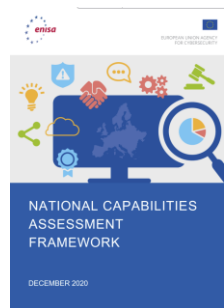
The National Cybersecurity Index (NCSI) is managed by the e-Governance Academy Foundation in Estonia. The index measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cybersecurity capacity building. Rankings are based on public evidence, specifically: 1) legal acts, 2) official documents, and 3) official websites.

Geographies: Global

BEST FOR: national assessments of cybersecurity capacity

National Capabilities Assessment Framework | European Union Agency for Cybersecurity (ENISA), 2020

[Link here](#)



The National Capabilities Assessment Framework (NCAF) aims at providing Member States with a self-assessment of their level of maturity by assessing their National Cybersecurity Strategy (NCSS) objectives, that will help them enhance and build cybersecurity capabilities both at strategic and at operational level. This framework was designed with the support of ENISA subject matter experts and representatives from 19 Member States and EFTA countries. The target audience of this report is policymakers, experts, and government officials responsible for or involved in designing, implementing, and evaluating an NCSS and, on a broader level, cybersecurity capabilities.

Geographies: European Union

BEST FOR: national assessments of cybersecurity capabilities

Continued on next page...

Examples of digital and cybersecurity assessment tools (continued)

Resource

Cybersecurity Capability Maturity Model (C2M2) | United States Department of Energy

[Link here](#)



Overview, focus and purpose

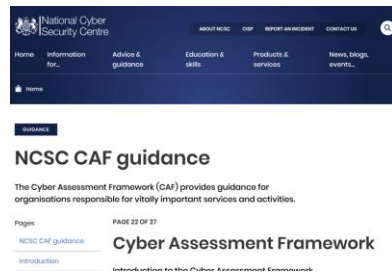
The Cybersecurity Capability Maturity Model (C2M2) is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology and operations technology assets and environments. The model can be used to: 1) strengthen organizations' cybersecurity capabilities; 2) enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities; 3) share knowledge, best practices, and relevant references across organizations to improve cybersecurity capabilities; and 4) enable organizations to prioritize actions and investments to improve cybersecurity.

Geographies: United States

BEST FOR: assessments of maturity at organizational level

Cyber Assessment Framework (CAF) | United Kingdom National Cybersecurity Centre, published in 2019 and last reviewed in 2022

[Link here](#)



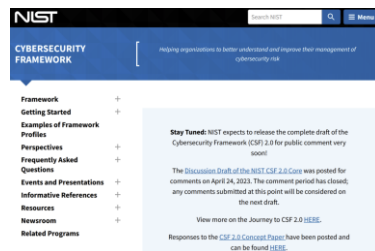
The Cyber Assessment Framework (CAF) provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organization responsible. It is intended to be used either by the responsible organization itself (self-assessment) or by an independent external entity, possibly a regulator or a suitably qualified organization acting on behalf of a regulator. The CAF collection consists of a set of 14 cybersecurity and resilience principles, together with guidance on using and applying the principles, and the Cyber Assessment Framework (CAF) itself.

Geographies: United Kingdom

BEST FOR: assessments of maturity for operators of critical activities

NIST Cybersecurity Framework | United States National Institute of Standards and Technology (NIST), last updated in 2018 (update underway)

[Link here](#)



The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. The Cybersecurity Framework consists of three main components: the Core provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand; the Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management; and the Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Though the Framework is not a one-size-fits-all approach, organizations can customize its practices.

Geographies: United States

BEST FOR: assessments of maturity at organizational level

Notes

- 1 Two illustrative examples of cybersecurity incidents in the health sector include a ransomware attack on a German hospital in 2020 (see [https://cyberlaw.ccdcoe.org/wiki/German_hospital_ransomware_attack_\(2020\)](https://cyberlaw.ccdcoe.org/wiki/German_hospital_ransomware_attack_(2020))) and a cyberattack on a Singaporean health database (see <https://www.reuters.com/article/us-singapore-cyberattack-idUSKBN1KA14J>)
- 2 See key findings of Sophos report on the State of Ransomware in Healthcare 2022 available from <https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare>.
- 3 See highlights of IBM's 2022 Cost of a Data Breach report available from <https://www.ibm.com/reports/data-breach>.
- 4 See CyberPeace Institute's Cyber Incident Tracer available from <https://cit.cyberpeaceinstitute.org/>.
- 5 This section is based extensively on (OECD 2022a).
- 6 See the World Bank's Cybersecurity Multi-Donor Fund, available from <https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview>.
- 7 See the Principles for Digital Development available from <https://digitalprinciples.org/principles/>; the World Bank Group endorsed these principles in 2016.
- 8 See the United States Cybersecurity Framework available from <https://www.nist.gov/cyberframework>.
- 9 See the Australian Victorian Department of Health's Digital Health's Health Sector Cyber Security Assessment available from <https://www.vmia.vic.gov.au/tools-and-insights/health-sector-cyber-security-assessment>.
- 10 See the United Kingdom's Commonwealth National Cyber Risk Assessments available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971015/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf.
- 11 See the European Union Risk Management Capability Assessment Guidelines available from [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808\(01\)&from=HU](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808(01)&from=HU).
- 12 (ENISA 2022) also provides a maturity model for CSIRTs that could be helpful for TTLs.
- 13 (ENISA 2021b) also provides a list of tools in service for CSIRTs (see table 5 in citation).
- 14 See Global Data Systems's Cyber Insurance Checklist: 12 Essential Security Controls available from <https://www.getgds.com/resources/blog/cybersecurity/cyber-insurance-checklist-12-essential-security-controls>.
- 15 See the World Bank's Cybersecurity Multi-Donor Fund, available from <https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview>.

References

- Akhlaq, Ather, Brian McKinstry, Khalid Bin Muhammad, and Aziz Sheikh. 2016. "Barriers and Facilitators to Health Information Exchange in Low- and Middle-Income Country Settings: A Systematic Review." *Health Policy and Planning* 31 (9): 1310–25. <https://doi.org/10.1093/heapol/czw056>.
- Bernat, L. 2021. "Enhancing the Digital Security of Critical Activities." Organisation for Economic Co-operation and Development (OECD). https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf.
- CISA. 2021. "Cybersecurity Perspectives: Healthcare and Public Health Response to COVID-19." Cybersecurity & Infrastructure Security Agency (CISA).
- Council of Europe (CoE), Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber, Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization, (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO, et al. 2021. "Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic Engagement in Cybersecurity." International Telecommunication Union. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf>.
- CyberPeace Institute. 2021. "Playing with Lives: Cyberattacks on Healthcare Are Attacks on People." CyberPeace Institute. <https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf>.
- ENISA. 2019. "ICT Security Certification Opportunities in the Healthcare Sector." European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/healthcare-certification>.
- . 2020. "Procurement Guidelines for Cybersecurity in Hospitals." European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>.
- . 2021a. "Cloud Security for Healthcare Services." European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services>.
- . 2021b. "CSIRT Capabilities in Healthcare Sector." European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector>.
- . 2022. "ENISA CSIRT Maturity Framework - Updated and Improved." European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework>.
- . 2023. "Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies." European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies>.

- Ferry, Andrew M., Matthew J. Davis, Ewa Rumprecht, Alexander L. Nigro, Priya Desai, and Larry H. Hollier. 2021. "Medical Documentation in Low- and Middle-Income Countries: Lessons Learned from Implementing Specialized Charting Software." *Plastic and Reconstructive Surgery Global Open* 9 (6): e3651. <https://doi.org/10.1097/GOX.0000000000003651>.
- FIRST.Org. 2019. "Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0." https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf.
- International Telecommunication Union. 2020. "Global Cybersecurity Index 2020." International Telecommunication Union (ITU).
- Ipsos. 2021. "Perspectives in Healthcare Security." https://www.ipsos.com/sites/default/files/ct/news/documents/2021-08/CyberMDX%20Philips_Perspectives%20in%20Healthcare%20Security.pdf.
- Marsh & McLennan Companies. 2018. "Holding Healthcare to Ransom - Industry Perspectives on Cyber Risks." https://www.marshmcclennan.com/content/dam/oliver-wyman/v2/publications/2018/september/holding-healthcare-to-ransom_sep18.pdf.
- Ngugi, Philomena, Ankica Babic, James Kariuki, Xenophon Santas, Violet Naanyu, and Martin C. Were. 2021. "Development of Standard Indicators to Assess Use of Electronic Health Record Systems Implemented in Low-and Medium-Income Countries." *PLOS ONE* 16 (1): e0244917. <https://doi.org/10.1371/journal.pone.0244917>.
- O'Brien, Niki, Guy Martin, Emilia Grass, Mike Durkin, and Saira Ghafur. 2020. "Safeguarding Our Healthcare Systems: A Global Framework for Cybersecurity."
- Odekunle, Florence Femi, Raphael Oluseun Odekunle, and Srinivasan Shankar. 2017. "Why Sub-Saharan Africa Lags in Electronic Health Record Adoption and Possible Strategies to Increase Its Adoption in This Region." *International Journal of Health Sciences* 11 (4).
- OECD. 2022a. *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*. Paris: Organisation for Economic Co-operation and Development. https://www.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en.
- . 2022b. *Recommendation of the Council on National Digital Security Strategies*. *OECD/LEGAL/0480*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480>.
- Price, Patricia, Richard Sullivan, Mykola Zubarev, and Ruslan Zelinskyi. 2022. "Radiotherapy in Conflict: Lessons from Ukraine." *The Lancet Oncology* 23 (7): 845–47. [https://doi.org/10.1016/S1470-2045\(22\)00298-4](https://doi.org/10.1016/S1470-2045(22)00298-4).
- Republic of Kenya. 2022. "National Cybersecurity Strategy." National Computer and Cybercrimes Coordination Committee (NC4) Secretariat. <https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf>.
- The Royal Australian College of General Practitioners. 2013. "Computer and Information Security Standards For General Practices and Other Office-Based Practices." <https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Practice%20sta>

ndards/Computer-and-information-security.pdf.

U.S. Department of Health and Human Services. 2023. "Health Care Sector Cybersecurity Framework Implementation Guide (Sector Guide)."

U.S. Department of Homeland Security and U.S. Department of Health and Human Services. 2016. "Healthcare and Public Health Sector-Specific Plan." <https://www.hsdl.org/c/abstract/>.

World Bank. 2020. "Digital Government Readiness Assessment (DGRA) Toolkit V.31 Guidelines for Task Teams." <https://openknowledge.worldbank.org/server/api/core/bitstreams/1d64ec08-4b54-5805-9900-63829e216e67/content>.

—. 2021. "Enhancing the Protection and Cyber-Resilience of Critical Information Infrastructure." Digital Regulation Platform. 2021. <https://digitalregulation.org>.

World Health Organization, and International Telecommunication Union. 2012. *National EHealth Strategy Toolkit*. International Telecommunication Union. <https://apps.who.int/iris/handle/10665/75211>.