Organisation for Economic Co-operation and Development

DELSA/HEA/WD/HWP(2023)16

Unclassified English text only

21 November 2023

DIRECTORATE FOR EMPLOYMENT, LABOUR AND SOCIAL AFFAIRS
HEALTH COMMITTEE

Health Working Papers

OECD Health Working Papers No. 164

FAST-TRACK ON DIGITAL SECURITY IN HEALTH

Eric SUTHERLAND*, Rishub KEELARA*, Samuel EISZELE* and June HAUGRUD*

JEL classification: H11, H40, H51, I18

Authorised for publication by Stefano Scarpetta, Director, Directorate for Employment, Labour and Social Affairs

(*) OECD, Directorate for Employment, Labour and Social Affairs, Health Division

.

All Health Working Papers are now available through the OECD Website at
https://www.oecd.org/health/health-working-papers.htm

JT03532204

OECD Health Working Papers

https://www.oecd.org/health/health-working-papers.htm

OECD Working Papers should not be reported as representing the official views of the OECD or of its member countries. The opinions expressed and arguments employed are those of the author(s)

Working Papers describe preliminary results or research in progress by the author(s) and are published to stimulate discussion on a broad range of issues on which the OECD works. Comments on Working Papers are welcomed and may be sent to health.contact@oecd.org.

This series is designed to make available to a wider readership selected health studies prepared for use within the OECD. Authorship is usually collective, but principal writers are named. The papers are generally available only in their original language – English or French – with a summary in the other.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Note by the Republic of Türkiye

The information in this document with reference to “Cyprus” relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Türkiye recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Türkiye shall preserve its position concerning the “Cyprus issue”.

Note by all the European Union Member States of the OECD and the European Union

The Republic of Cyprus is recognised by all members of the United Nations with the exception of Türkiye. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

Acknowledgements

The work presented here was undertaken by Eric Sutherland, Rishub Keelara, June Haugrud, and Samuel Eiszele. The authors would also like to thank Peter Stephens and colleagues from the OECD Directorate for Science, Technology, & Innovation (OECD/STI) for their advice and guidance with the analyses.

The views expressed in this document are those of the authors and not necessarily the views of any OECD country, individual expert, or the European Union.

Abstract

In response to the increase of cyberattacks in health care setting, the Health Committee of the OECD asked for a fast-track report on Digital Security as part of the OECD ongoing work on health data governance. The OECD published a framework for digital security risk management in December 2022, addressing the growing concern of digital security risks in the healthcare sector. The report emphasized that as the healthcare industry undergoes digital transformation, it brings significant benefits while simultaneously escalating the vulnerability to cyber threats. These digital security breaches can have dire consequences on healthcare, as the sector increasingly relies on digital tools for patient care and telemedicine, a reliance that surged during the COVID-19 pandemic.

Recognizing the gravity of the situation, several OECD countries, including Norway, Czechia, Ireland, Canada, the United Kingdom, and Costa Rica, have experienced disruptions in healthcare services due to cyberattacks. As a response, the OECD introduced a Digital Security Risk Management Framework in 2022, featuring nine principles aimed at enhancing digital security culture, responsibility, transparency, cooperation, and strategic integration.

This Working Paper investigated a questionnaire based on these principles which has revealed varying levels of digital security alignment among countries, with Ireland and Korea exhibiting full alignment. Notably, countries with specific strategies for digital security in health showed higher alignment to leading practices. This Working Paper identified key areas for improvement, including fostering a digital security culture through training, strengthening strategy and governance, and embedding risk assessment and treatment.

The report also emphasizes the need for collaboration on innovative tools to detect and manage digital security threats, such as multi-factor authentication and encryption. These collaborative efforts are essential to safeguard the digital foundations of modern healthcare systems and ensure the security of health data and services.

Résumé

Face à l'augmentation des cyberattaques dans le secteur de la santé, le Comité de la santé de l'OCDE a demandé un rapport accéléré sur la sécurité numérique dans le cadre des travaux en cours de l'OCDE sur la gouvernance des données de santé. L'OCDE a publié en décembre 2022 un cadre pour la gestion des risques liés à la sécurité numérique, qui répond aux préoccupations croissantes concernant les risques liés à la sécurité numérique dans le secteur des soins de santé. Le rapport souligne que la transformation numérique du secteur de la santé apporte des avantages significatifs tout en augmentant la vulnérabilité aux cybermenaces. Ces atteintes à la sécurité numérique peuvent avoir des conséquences désastreuses sur les soins de santé, car le secteur s'appuie de plus en plus sur des outils numériques pour la prise en charge des patients et la télémédecine, une dépendance qui s'est accrue pendant la pandémie de COVID-19.

Conscients de la gravité de la situation, plusieurs pays de l'OCDE, dont la Norvège, la Tchéquie, l'Irlande, le Canada, le Royaume-Uni et le Costa Rica, ont connu des perturbations des services de santé en raison de cyberattaques. En réponse à cette problématique, l'OCDE a introduit en 2022 un Cadre de gestion des risques liés à la sécurité numérique, qui comprend neuf principes visant à renforcer la culture de la sécurité numérique, la responsabilité, la transparence, la coopération et l'intégration stratégique.

Ce document de travail a analysé un questionnaire basé sur ces principes, qui a révélé des niveaux variables d'alignement de la sécurité numérique entre les pays, avec l'Irlande et la Corée affichant un alignement entier. En particulier, les pays qui ont mis en place des stratégies spécifiques pour la sécurité numérique dans le domaine de la santé se sont davantage alignés sur les pratiques de pointe. Ce document de travail a identifié des domaines clés à améliorer, notamment la promotion d'une culture de la sécurité numérique par la formation, le renforcement de la stratégie et de la gouvernance, et l'intégration de l'évaluation et du traitement des risques.

Le rapport souligne également la nécessité de collaborer autour d'outils innovants pour détecter et gérer les menaces à la sécurité numérique, tels que l'authentification multifactorielle et le cryptage. Ces efforts de collaboration sont essentiels pour préserver les fondements numériques des systèmes de santé modernes et garantir la sécurité des données et des services de santé.

Table of contents

TABLES

In Brief

Key Findings

1. The digital transformation of the healthcare sector brings significant benefit to individuals, communities, and the public sector; however, it also increases the risk of digital security threats. Across all industries, cyberattacks are on track to cause USD$10.5 trillion a year in damage by 2025.

2. Disruptions caused by digital security breaches can have a severe impact on health. Given the digitalisation of health services – which rapidly increased during COVID-19 – there is significant reliance on the ability to access health data for the provision of care and on the use of technology to engage in telemedicine. Cyberhackers exploit human and technical vulnerabilities to ultimately disrupt or deny the use of digital technologies and preventing access to health data – their intent is to secure a ransom in exchange for restoring reliable access to data and technology. During these disruptions, health outcomes may suffer as health services that rely on digital tools and health data suffer when they are suddenly unavailable. Economically, there are significant expenses related to addressing a security breach, related to remediating all computing technologies.

3. Several OECD countries have recently experienced disruption in health services due to cyberattacks including Norway (in 2018), Czechia (in 2020), Ireland (in 2021), Canada (in 2021), United Kingdom (in 2022), and Costa Rica (in 2022), among others. Recognizing the increasing risk, the Health Committee asked the OECD Health Division to write a fast-track analysis of the current state of digital security in health.

4. Use case studies, such as the example of Costa Rica who provided a deep dive into their May 2022 cyberattack and response, demonstrate the real implications of cyberthreats to negatively impact health systems. More than 60,000 computers were impacted and cleansing all the machines took four months during the busiest time of the year for Costa Rica. The significant disruption caused dissatisfaction with health services, although it did raise awareness of the importance of digital tools.

5. The OECD published a Digital Security Risk Management Framework in 2022, which included nine principles for digital security, which are consistent with the OECD Recommendation on Health Data Governance (2017). With these principles, all stakeholders should:

- create a culture of digital security based on the understanding of digital security risk and how to manage it;
- take responsibility for the management of digital security risk based on their roles, the context, and their ability to act;
- manage digital security risk in a transparent manner and consistently with human rights and fundamental values; and
- co-operate, including across borders.

6. The principles also indicate leaders and decision makers should ensure that:

- digital security risk is integrated in their overall risk management strategy and managed as a strategic risk requiring operational measures;
- digital security risk is treated based on continuous risk assessment;

- security measures are appropriate to and commensurate with the risk;
- a preparedness and continuity plan based on digital security risk assessment is adopted, implemented, and tested, to ensure resilience; and
- innovation is considered.

7. These digital security risk management principles were used as the basis for the fast-track questionnaire and analysis. Twenty-five countries responded to the questionnaire.

8. While all countries recognise the importance of digital security as part of their overall program of work, there was variation in the frequency, scope, and level of co-operation for digital security risk management.

9. Responses in the questionnaire were compared with leading practice, such as identifying a clear lead to digital security in health that works across health organisations, other industries, and international partners to detect and understand digital security threats and work together to act in case of an attack. Overall, 75% of responses were aligned with identified leading practice. **Ireland** and **Korea** were the only OECD countries that are fully aligned across all nine digital security principles. Countries that had a **specific strategy for digital security in health** – including Australia, Canada, Czechia, France, Germany, Ireland, Israel, Netherlands, Norway, the United Kingdom and the United States – were aligned to the digital security risk management principles in an average of 6.1 of 9 principle areas. This was a higher alignment than countries with only a national strategy in digital security (4.7 of 9) or no strategy (4.5 of 9).

10. The analysis shows some key priority areas for governmental action to align with the OECD Digital Security Risk Management Framework and cooperate in areas of mutual benefit. These include:

1. improving digital security culture, for example by promoting a culture of digital security through initial and refresher training programs for all employees as well as periodic phishing simulations as done in Israel and cyberattack simulations as done in Korea;
2. strengthening strategy and governance, as in Australia where managing digital security risk in health is part of an overall approach to risk management and at least 10% of IT budgets allocated to digital security (which is in line with other industries); and
3. embedding risk assessment and treatment, for example by monitoring and reporting the effectiveness of the digital security program at least quarterly to ensure that digital security risks are always top of mind. Korea surpasses this practice through monthly reporting.

11. It is notable that some areas for improvement to mitigate digital security risks are relatively low-cost (such as training staff and monitoring programs) when compared to extensive interventions such as advanced security solutions, security audits and penetration testing, amongst others. It is estimated that 90% of digital security challenges start with phishing. Hence these low-cost activities could also be among the most effective.

12. There is also a need for further collaboration on innovation and emerging tools for threat detection and security management. Common innovations being implemented are identity management, multi-factor authentication, role-based access, and applying encryption for data at rest and in motion. Emerging tools are being investigated across the OECD including zero-trust approaches (in Norway), synthetic data (in Israel), applying Block Chain (in Korea), and Cloud technology (in Ireland and Netherlands).

1. Introduction to digital security

13. With the increasing digitisation of society, it is inevitable that digital security[1] threats will also increase. In health, digitalisation is accelerating as the sector seeks to be patient-centric, increase efficiency, reduce costs, advance research, and improve collaboration. Examples of digitalisation are the implementation of tools for appointment management, technologies for remote monitoring and care, and the use of big data analytics and artificial intelligence in health. The accelerating digital transformation leaves health systems vulnerable to new challenges in digital security that extract value from health data assets or prevent their use in care.

14. Criminal and state-sponsored actors are scaling up their nefarious actions for financial, political, and geopolitical gains, among others. While there is no consensus on methodology for estimating the cost of cyberattacks, recent research suggests that the cost ranges from USD$100 billion to USD$6 trillion annually and rising every year (OECD, 2021[1]), with some projections that the cost will rise to USD$10.5 trillion by 2025 across all industries (Mckinsey and Company, 2023[2]). Furthermore, in the first three months of 2023, there have been more attempted cyberattacks than in all of 2022.

15. Organisations have not always sufficiently assessed the digital security risk incurred by this evolution, nor taken proportionate security measures to manage it. Individuals are confused by complex cyber security technical jargon, settings, and procedures such as updates, authentication processes, and encryption among others. Products and services are not sufficiently secure and expose users to security risk without giving them appropriate information and means to mitigate them (OECD, 2022[3]).

16. The next sub-section provides an overview of the OECD legal instrument for Digital Security Risk Management, which was used as the basis for this fast-track questionnaire and analysis.

17. Section 2 emphasises the importance of digital security in health and the linkages between the approach for digital security risk management and the OECD Recommendation on Health Data Governance (2017[4])

18. Section 3 provides a summary of country responses to their approach to digital security in health based on their experience during the COVID-19 pandemic. The end of Section 3. provides a target state for digital security in health and examines alignment of respondents to that target state.

19. Section 4. identifies opportunities for individual and collective actions to foster coordination, cooperation, and collaboration within and across OECD countries to fortify the foundation of digital security risk management.

[1] Digital security is defined as “the set of measures taken to manage digital security risk for economic and social prosperity.” ([6])

1.1. OECD Legal Instrument on Digital Security Risk Management

20. Counter-intuitively, major digital security challenges are not technical. According to Deloitte, 90% of successful cyberattacks start with phishing[2] (Deloitte, 2020[5]). The best defence to such attacks is preparedness, training, and communication.

21. Recognising the non-technical nature of digital security, the OECD published a framework for digital security risk management in December 2022 (OECD, 2022[3]) to assist countries to understand and mitigate digital security risks. The recommendations highlight that with the growing sophistication and number of cyberattacks, governments should adopt a formal and structured approach to evaluate and mitigate digital security risks that minimises the likelihood and impact of successful cyberattacks. In the OECD recommendations, there are nine guiding principles for the foundational layer of digital security risk management (Table 1.1).

Table 1.1. OECD Digital Security Risk Management Guiding Principles

Principle		Description
1.	Digital Security Culture: Awareness, skills, and empowerment	All stakeholders should create a culture of digital security based on the understanding of digital security risk and how to manage it.
2.	Responsibility and Liability	All stakeholders should take responsibility for the management of digital security risk based on their roles, the context, and their ability to act.
3.	Human rights and fundamental values	All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.
4.	Co-operation	All stakeholders should co-operate, including across borders
5.	Strategy and Governance	Leaders and decision makers should ensure that digital security risk is integrated in their overall risk management strategy and managed as a strategic risk requiring operational measures.
6.	Risk assessment and treatment	Leaders and decision makers should ensure that digital security risk is treated based on continuous risk assessment.
7.	Security Measures	Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.
8.	Resilience, preparedness & continuity	Leaders and decision makers should ensure that a preparedness and continuity plan based on digital security risk assessment is adopted, implemented, and tested, to ensure resilience.
9.	Innovation	Leaders and decision makers should ensure that innovation is considered.

Note the table is an abstract, in which each principle includes more provisions and detail in the policy framework.
Source: OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. ([6])

22. The guiding principles in Table 1.1 are not specific to health; however, are appropriate for consideration in health. In comparison to the Recommendation on Health Data Governance (OECD, 2017[4]), these principles are fully aligned (Table 1.2) and provide more detail for an assessment on digital security.

[2] Phishing is where a fraudulent email is sent to entice the employee to click a link and that link enable the cyberattacker inappropriate access to the organisations technology systems.

Table 1.2. OECD Recommendation on Health Data Governance and Digital Security

Cross-reference: OECD Recommendation on Health Data Governance and Digital Security Risk Management Framework

OECD Recommendation on Health Data Governance	Reference to Security	Alignment to OECD Digital Security Risk Management Framework
2. Co-ordination and cooperation	Encourage common policies and procedures that minimise barriers to sharing data for health system management, statistics, research, and other health-related purposes that serve the public interest while protecting privacy **and data security.**	4. Co-operation
3. Capacity	Review capacity to process personal health data and protect the public interest including data availability, quality, fitness for use, accessibility, as well as privacy and **data security protections.**	1. Digital Security Culture: Awareness, skills, and empowerment
7. Transparency	Transparency through public information mechanisms which do not compromise health data privacy **and security protections** or organisations' commercial or other legitimate interests	3. Human rights and fundamental values
8. Maximising use of technology	Enabling the availability, re-use, and analysis of personal health data while, at the same time, protecting privacy and **security** and facilitating individuals' control of the uses of their own data.	9. Innovation
9. Monitoring and evaluation	Periodic assessment and updating of policies and practices to manage privacy, protection of personal health data and **security risks** relating to personal health data governance.	6. Risk assessment and treatment
10. Training and skills development	Establishment of appropriate training and skills development in privacy and **security measures** for those processing personal health data,	2. Responsibility and Liability
11. Controls and safeguards	Establish requirements that personal health data can only be processed by, or be the responsibility of, organisations with appropriate data privacy and **security** training for all staff members Encourage organisations processing personal health data to designate an employee or employees to coordinate and be accountable for the organisation's information **security** programme Include technological, physical, and organisational measures designed to protect privacy and **security**	5. Strategy and Governance 7. Security Measures 8. Resilience, preparedness & continuity

Source: OECD Recommendation on Health Data Governance ((OECD, 2017[4]))

2. Increasing digital security threats in health

23. Across the OECD, there have been many significant disruptions in health services due to cyberattacks including in **Norway** (2018), **Czechia** (2020), **Ireland** (2021), **Canada** (2021) and **Costa Rica** (2022 – see Box 2.1 on page 13) (Hughes, 2018[7]; Solomon, 2023[8]; Stephends, 2020[9]; Tidy, 2021[10]).

24. In 2020, the **German** government reported a doubling of cyberattacks. In 2022, there were 27 reported security breaches in **France**. In the **United Kingdom**, the National Cyber Security Centre reported mitigating 777 incidents in 2022 (Witts, 2023[11]). In the **United States of America**, there were a reported 1,410 *weekly* cyberattacks *per organisation* in 2022, an increase of 86% over the previous year (Anderson, 2023[12]).

25. Disruptions caused by digital security breaches can have severe health and economic impacts. Cyberhackers exploit human and technical vulnerabilities to ultimately deny the use of digital technologies and preventing access to health data through encryption. They ask for a ransom in exchange for restoring access to data and technology (known as ransomware). In 2020, 34% of healthcare organisations reported being affected by ransomware, 65% of those reporting that cybercriminals were successful in encrypting data. During these disruptions, health outcomes may suffer where health services rely on digital tools and health data by temporary reversion to manual paper-based workflows that slows care, increases wait times, and exhausts health workers.

26. Economically, there are significant expenses to address the security breach. The average cost of remediating a ransomware attack has been estimated to be between US$1.27 million to US$4.6 million per incident. When hospitals have been impacted, a cyber incident resulting in a shutdown can cost between US$21,500 to US$47,500 *per hour* (Witts, 2023[11]).

27. Gaining access to valuable and sensitive health data is also a target of cybercrime where the value of a personally identifiable health record is higher than other industries (US$180 vs US $161). Healthcare related data breaches were reported to cost US$21 billion in 2020. This is projected to grow in the next three years to US$6 trillion (Sobers, 2022[13]). while there is no broadly accepted methodology for estimating the cost and impact of digital security, it is clear from the above that threats are real and expected to increase.

28. Addressing digital security in health has been a focus of the OECD has been a focus for several years, with priority on security included in the OECD Recommendation on Health Data Governance and health explicitly identified as a 'critical activity' in the OECD Recommendation on Digital Security for Critical Activities (2019). Table 1.2 demonstrates the relationship between the OECD Recommendations on Digital Security Risk Management and Health Data Governance that validates their alignment.

29. With that in mind in June 2022 the OECD was tasked by the Health Committee to author a Fast-Track paper on Digital Security in Health. This fast-track analysis is based on responses to a questionnaire that was distributed to Health Committee in January 2023.

Box 2.1. Costa Rica experiences a cyberattack

30. Costa Rica's public health care services experienced a cyberattack during the night on Monday May 31st, 2022. The event started, like out of a horror movie, when all the printers in one Costa Rican hospital began printing a ransom note (for $5MM USD). Consequently, their ability to use their systems was compromised. They had been the victim of a cyber security attack caused by a computer virus.

31. On being notified of the event, the institution enacted their response. The first step was to disconnect all their systems to contain the issue and minimise risk of an information breach. The second step was to assess impacts and determine actions so that the computers could be reconnected to the network to be able to access and share data. As the problem was investigated, it was determined that there was risk of infection in more than 60,000 computers. Fortunately, there was no privacy breach of personal health information.

32. Remedial action was necessary to clean up each of those computers to remove the virus and improve security controls. That process occurred during what has historically been Costa Rica's busiest period of the year from June to October.

33. The impact of disconnecting all the institutional systems were immense including a significant negative impact on health services and growing frustration among the public. This was especially since public health care services are the largest provider of health services in the country with a national network of clinics and hospitals spread countrywide. During the remedial action, providers and patients could not access comprehensive electronic medical records, appointments were recorded by hand, and mobile phones were used to share information with each other. The sudden reversion to the pre-digital age increased awareness of the value that integrated technology provides providers and the public.

34. To address the incident, and be more resilient to future attacks, several changes were introduced. This included upgrading security software, increasing security training for all employees, hiring security expertise, establishing backup data centres, and providing clarity on digital health policy and technical requirements. Government would set the rules (e.g., legislation, technical standards) for digital security and support institutions as those policies were implemented in local context.

35. There are many positive lessons learned from the Costa Rican cyberattack. The response by the Costa Rican authorities and technicians demonstrated the value of planning and preparedness. The response was complex and involved many stakeholders. This emphasised the need for orchestration across the public- and private-sector as well as with the public. The value of cross-border cooperation was also highlighted as Spain and the United States both helped in the response. The Costa Rican government also made sure other departments and countries knew of their incident to prevent the further spread of the same virus.

36. In the aftermath of the cyberattack, the Costa Rican government evaluated their response and invested in digital security for health. Their experience demonstrates the value of preparedness, cooperation, and diligence to minimise likelihood and impact of future digital security incidents.

Note: Based on interviews with Costa Rica's Dirección de Servicios de Salud

3. Approach to digital security in health across OECD countries

37. The use of health data and digital health services during the COVID-19 pandemic has illustrated how a digital transformation of healthcare can lead to significant benefits. It also revealed health systems' increasing reliance on information and communication technologies for critical activities. Health systems are especially vulnerable to digital security threats for many reasons, including the ubiquitous use of interconnected medical devices, patients', and health workers' use of digital devices for accessing health data, the perceived value of both identified and de-identified health data, and limited health budgets for cybersecurity.

38. To help understand and mitigate digital security risk, a questionnaire for digital security in health was shared in January 2023. The questionnaire was in two parts. The first part of the questionnaire asks countries broad questions on the approach to digital security in health. The second part of the questionnaire examined specific COVID-19-related use cases with respect to the guiding principles from the OECD Digital Security Risk Management framework (OECD, 2022[14]). The use cases asked respondents to identify specific systems that would be used for later responses.

39. Twenty-five countries (Croatia and twenty-four OECD countries) replied to the questionnaire. Practically, responses to the second part were similar across all use cases. As such, in the summary below, they are presented together with nuances articulated where appropriate. Further, some countries declined to respond to some of the questions on the basis that the answers were confidential and could inadvertently increase their digital security risk in health.

40. The following sub-sections summarise responses to each of these parts, including detailed summaries for each of the nine guiding principles. This section concludes with a high-level synthesis.

3.1. Overall strategies for digital security in health

41. OECD countries have different strategic approaches to digital security in health. Of responding countries, eleven have a national health-specific strategy for digital security (of which six align with a whole-of-government digital strategy). Ten countries have a national strategy for digital security, however, have not indicated that this is specific to health. Four countries indicated that there is no formalised approach to digital security in health at a national level; however, these countries have addressed specific aspects of digital security risk management and have comprehensive plans to secure health data. (Table 3.1)

Table 3.1. Framework for National Digital Security in Health

11		
Australia	10	
Canada	Costa Rica	
Czechia	Croatia	
France	Italy	
Germany	Japan	
Ireland	Korea	
Israel	Lithuania	4
Netherlands	Portugal	Belgium
Norway	Slovenia	Greece
United Kingdom	Spain	Luxembourg
United States	Switzerland	Slovak Republic
Digital security strategy specific to health (bolded countries identified alignment with a national digital health strategy)	**National strategy for digital security**	**Did not report a national approach to digital security**

Source: OECD 2023 Digital Health Security questionnaire.

42. **Australia, Canada, Czechia, Netherlands, and the United Kingdom** indicated that there is a digital security framework that is specific to health. Further to this, **France**, **Germany**, **Ireland**, **Israel**, **Norway**, and the **United States** indicated that there is a digital security framework for health and that this framework is aligned with an overall national approach to digital security. **Germany** explained it was not feasible to provide uniform answers due to healthcare provider diversity, criticalities, and IT usage variations within their security framework. **Australia** noted that, as accountability for health is at the state / territory level, the authority to implement and manage digital security in health services rests with them. Additionally, **The United Kingdom** recently launched (March 2023) a cyber security strategy for digital health.

43. **Costa Rica, Croatia, Italy**, **Japan**, **Korea**, **Lithuania**, **Portugal**, **Slovenia**, **Spain,** and **Switzerland** rely on a national cybersecurity framework rather than having a strategy specific to health. In **Costa Rica** and **Italy,** all digital technologies in the public sector are under the same legal framework. In **Portugal**, there are several laws and regulations governing the use and protection of information systems and networks, including both national and transnational (EU) laws and regulations. Similarly, in **Croatia** and **Switzerland,** laws and regulations govern all projects, with projects being managed according to their security risk rating. Finally, **Slovenia** has information security incorporated in most national strategies.

44. Four countries (**Belgium, Greece, Luxembourg,** and the **Slovak Republic**) did not report any national approach to digital security in health. Through their responses, these countries have identified concrete plans and regulations for digital security in health, although not part of a coherent national plan.

3.2. Approaches to digital security in health across OECD countries

45. The OECD Recommendation on Digital Security Risk Management presents nine principles for effective digital security risk management. These principles are complementary and coherent, covering risk mitigations across people (culture and training, co-operation, responsibility), governance (strategy, risk assessment, transparency, preparedness), and technology (innovation, security measures).

46. Risk mitigations related to people seek to create a culture of digital security where individuals understand their role and responsibility in digital security risk management. Given that the majority of cyberattacks start with phishing, this area is important in preventing successful cyberattacks. Further, people risk mitigations foster a culture of cooperation that is important in minimising the impact and duration of a cybersecurity incident.

47. Governance risk mitigations clarify strategic priorities for security risk management while achieving broader health system objectives. Governance also provides financial resources, identifies risks, develops risk mitigation plans, and prepares for future incidents to minimise likelihood and lower impact of security breaches. Finally, governance evaluates the security program and transparently communicates among all stakeholders. Governance is essential for the long-term resilience of the digital security risk management program to ensure responses are coherent and comprehensive across the health system.

48. Technology risk mitigations provide the tools and technologies to protect against cyberthreats, continually innovating to develop new security measures as well as applying known fixes. Keeping on top of security patches is an essential part of a risk management program. When technologies are not patched, they can have severe impacts across an entire network as learned by the WannaCry attack in 2017, which cost US$4 billion in losses globally as the virus spread. (See Table 3.1)

49. It is notable that most actions for digital security risk management relate to people and governance rather than technology. All are important in the context of a robust risk management program. This section will summarise responses to specific areas of the questionnaire organised by the nine principles in the OECD digital security framework as summarised in Table 1.1. Each section includes context for the importance of the principle.

Box 3.1. Global WannaCry Ransomware disrupted care for NHS England in 2017

50. The United Kingdom experienced the 'Wannacry' cyberattack in May 2017 which directly affected 1% of National Health Service (NHS) activity and disrupted the operations of 1/3 of hospital trusts. 8% of GP practices in the NHS were infected.

51. The WannaCry ransomware exploited a vulnerability in Microsoft Windows XP which could have been addressed by applying a security patch that had been identified two months prior to the attack. Unfortunately, the 80 NHS organisations that were affected did not apply the update patch to some of their computers running Microsoft XP, leaving them vulnerable to the ransomware. The ransomware demanded payment random payment in Bitcoin cryptocurrency and threatened to permanently delete files if not paid within three days.

52. Affected computers were unable to be used. Some critical medical devices and equipment that continue to use Microsoft XP were also affected, such as MRI scanners, CT scanners, blood test analysis devices, or any other devices that required Microsoft XP to access results or necessary software.

53. Back-up processes such as the NHS' "mutual aid" process were immediately enacted, in which an acute care facility that could no longer take patients would have another nearby facility take up the demand. The same evening of the attack, a 'kill switch' was discovered, which halted the ransomware from spreading further. From there, several NHS departments collaborated to coordinate response, information, and restoration of services, as well as to address any vulnerabilities in the system due to the act. This included releasing NHS-wide communications and guidance and requesting information from all NHS trusts.

54. The issue and solution were broadly communicated, and the problem was resolved after one week, without any ransom being paid. People providing clear communication and taking decisive action resulted in no harms to patients or breach of patient data. The incident highlighted to the NHS and individual NHS organisations the continued importance of building cyber resilience and the need to further fortify efforts to defend against future attacks. NHS England's Data Security Leadership Board agreed on a single coordinated resilience program shortly after the attack. In addition, a "Cyber Handbook" was produced to outline the actions to be taken in the event of another cyber-attack affecting the NHS. The encounter was quite costly for the NHS, with an estimated cost of £92 million. In addition, care for patients country-wide was halted or disrupted, with thousands of cancelled hospital and GP appointments, delayed social care, and effects on ambulances and emergency departments' ability to serve patients.

55. The 'Wannacry' attack spread internationally across all industries. It is estimated that the WannaCry ransomware has attacked around 230,000 computers globally, with an estimated monetary impact of US$4 billion in losses worldwide.

Source: (Smart, 2018[15]; kaspersky, n.d.[16])

3.2.1. Digital Security Culture: Awareness, skills, and empowerment

56. A culture of digital security is the most impactful defence to cyberthreats. According to a Deloitte report from 2020, 91% of all cyber-attacks begin with a phishing email to an unexpected victim. Overall, 32% of successful attacks involve phishing in some way (Deloitte, 2020[5]).

57. Respondents were asked to share their approach, so the health workforce is aware, skilled, and empowered to address threats. (Table 3.2)

Table 3.2. Digital Security Training and Awareness among Staff and Data Handlers

	Training of staff	Refreshment of training	Common curriculum	Pro-active measures	Types of pro-active measures
Australia	Yes	Yes*	Yes	Yes	Phishing simulations, refresh training, awareness, and other engagements
Belgium	Yes	Partly	No	Yes	Regular topic in monthly meeting
Canada	Yes	Partly	Yes	Yes	Phishing stimulations, security awareness and guidance
Costa Rica	Yes	Partly	No	Yes	Awareness
Croatia	Yes	No	No	Yes	Awareness
Czechia	Yes	Yes	Yes	No	n.a.
France	Yes	n.r.	Yes	n.r.	n.r.
Germany	n.r.	n.r.	n.r.	n.r.	n.r.
Greece	Yes	Yes	Yes	Yes	Essential training, awareness messages, threat information from specific information security forums
Ireland	Yes	Yes	Yes	Yes	Phishing stimulations, continuous monitoring, and awareness
Israel	Yes	Yes	Yes	Yes	Phishing simulations, reporting and awareness
Italy	No**	-	No**	Yes	Refresh training, cyber pills, and awareness
Japan	Yes	Yes	n.r	Yes	Simulation training
Korea	Yes	Yes	Yes	Yes	Education, training, vulnerability checks, simulation exercise
Lithuania	Yes	Yes	No	Yes	Training
Luxembourg	Yes	Yes	Partly	Yes	Staff meeting (monthly), awareness
Netherlands	Yes	Yes	No	Yes	Open communication, regular (weekly) staff meetings
Norway	Yes	Yes	Yes	Yes	Regular e-learning, awareness
Portugal	Yes	No	Yes	Yes	Documents
Slovak Republic	Yes	Yes	No	Yes	Monitoring, official periodic audit
Slovenia	Yes	Yes	No	Yes	Training and awareness
Spain	Yes	Yes	Yes	Yes	Security pills
Switzerland	Yes	No	No	No	n.a.
The United Kingdom	Yes	Yes	Yes	Yes	Training, campaigns, and phishing
The United States	Yes	Partly	n.a	Yes	Awareness, training and safeguard of passwords

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news, ** is currently being implemented, *Variation between private and public organisations
Source: OECD 2023 Digital Health Security questionnaire.

58. **Twenty-three** respondents reported mandatory security training of staff when coming into organisations responsible for health data processing. This includes **Australia, Belgium, Canada, Costa Rica, Croatia, Czechia, France, Greece, Ireland, Israel, Japan, Korea, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Slovenia, Spain, Switzerland, the United Kingdom,** and **the United States**. **Italy** reported not having a mandatory training requirement, although they are currently working on implementing a training and awareness program for Ministry of Health staff.

59. Refresher training varies from country to country. **Israel** and **Luxembourg** provide monthly refreshment; **Greece**, **Korea** and the **Slovak Republic** refresh training at least twice a year; **Australia**, **Ireland**, **Japan**, **Netherlands**, **Norway**, **Slovenia, Spain** and **the United Kingdom** provide annual training; and **Belgium, Canada**, **Croatia**, **Portugal** and **Switzerland** only provide onboarding training; however, **Belgium** keeps information available on the intranet, **Canada** and **Costa Rica** provide self-service training tools for their employees. **France** has included digital security in the curriculum of health-related higher education and **the United States** have no prescribed frequency or required onboarding training, though it is assumed security training is a part of onboarding.

60. Twelve countries (**Australia, Canada, Czechia, France, Greece, Ireland, Israel, Korea, Norway, Portugal, Spain, and the United Kingdom**) report that they have developed and implemented a common curriculum for all organisations. **Australia** has clarified that while the Australian Digital Health Agency has developed a common curriculum that is available for all healthcare organisations, that this is not mandatory to be used or implemented. **Lithuania**, which does not have a common curriculum, reports that training is mostly based on international programmes/courses. In **Switzerland** and **Scotland**, each organisation produces its own curriculum for data security. **Luxembourg** has a common curriculum for their main service (eSante), but not for their COVID Systems. **Italy** is currently rolling out a common guide for electronic health records.

61. Countries reported a variety of pro-active measures in place to support a culture of digital security in health. Examples include cyberattack simulations, awareness campaigns (e.g., Digital Security Month), regular refresh of training, and frequent discussions of the importance of security at staff meetings. The most frequent measure was phishing simulations where a fake email is sent internally so staff know what a phishing attack may look like and know what to do when they suspect a phishing attack.

62. Overall, respondents demonstrated strong alignment with the principle of Digital Security Culture. There is mandatory security training at onboarding, periodic updates to training to incorporate updates to defend against cyberthreats and learning about pro-active measures to build a culture of digital security in health.

3.2.2. Responsibility and Liability

63. Health systems are becoming increasingly digitised and interconnected. With the proliferation of the digital health ecosystem, it is more complex to detect, respond, contain, and remediate cyberattacks and how organisations coordinate their response. In digital health, organisations are connected in a series of data supply chains – and the security of that supply chain is only as strong as its weakest link. Clarifying accountability and responsibility across organisations is necessary to ensure ongoing successful operations, timely notification, and effective response.

64. Respondents were asked to share their approach to accountability and coordination across their health organisations. (Table 3.3)

Table 3.3. Coordination and accountability for digital security in health

	Defined responsibilities (e.g., key roles)	Aligning program for digital health security	Coordination actor or institution	
Australia	Yes	Yes	Yes	Federal Government and Cyber Security Centre
Belgium	Yes	Yes	Partly	n.r.
Canada	Yes	No	Yes	Government of Canada Policy
Costa Rica	Partly	No	Partly	Ministry of Science and Technology
Croatia	Yes	Yes	Yes	National Security Council framework
Czechia	Yes	Yes	Yes	National Cyber and Information Security Agency
France				
Germany				
Greece	Yes	Yes	Yes	Ministry of Digital Governance
Ireland	Yes	Yes	Yes	Health Service Executive (HSE)
Israel	Yes	Yes	Yes	Ministry of Health and National Cyber Directorate
Italy	Yes	Yes	Yes	n.r.
Japan	Yes	Yes	Yes	n.r.
Korea	Yes	Yes	Yes	Internal - department of information security
Lithuania	Yes	Yes	Yes	National Cyber Security Center
Luxembourg	Yes	Yes	Yes	Organ for secure information
Netherlands	Yes	Partly	Yes	Ministry of Health, Welfare, and Sports
Norway	Yes	Yes	Yes	The Norwegian Digitalisation Agency and Directorate for e-Health
Portugal	Yes	Yes	Yes	Coordinator Council of Information Security in Health
Slovak Republic	Yes	No	No	-
Slovenia	Yes	Partly	Yes	Government Information Security Office, Ministry of Health, and National Institute of Public Health
Spain	Yes	Yes	Yes	National Cryptology Centre
Switzerland	Yes	Yes	Yes	National Cyber Security Center
The United Kingdom	Yes	Yes	Yes	Security of Network and Information System Regulations and Government Health and Social Care Directorates
The United States	Yes	Yes	Yes	HIPAA Security Rule

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented
Source: OECD 2023 Digital Health Security questionnaire.

65. Countries report policies that define roles and responsibilities within public sector organisations handling health data. The titles of such roles vary: Chief Information Security Officer (**Australia, Ireland,** and **Netherlands**), Designated Official for Cyber Security (**Canada**), Information security consultants (**Slovenia**) Chief Information Security Officer (**Australia**), Cyber Security Manager (**Korea**), Security administrators (**Italy**), Coordinating Information Security Officer (**Lithuania**), IT director (**Norway**), Information Security Manager (**Portugal**). **Costa Rica** reports having partially defined roles in digital security and notes that there is an IT security unit that oversees the technical components of digital security; however, there are no unit in charge of information security at the business level within health.

66. Eighteen countries also identified programs to align digital security approaches across organisations, many of which pointed to policies and legislation regulating the organisation that process health data, which would support alignment of peer organisations.

67. Twenty countries identified an institution to lead coordination and alignment of programs for digital security in health. The institution guide adoption of leading practices. Many of these are national units for cyber and information security. In **Israel** and **Slovenia,** the Ministry of Health coordinates alignment of programs across health organisations. **Belgium** has minimum norms to receive authorisation from certain government bodies and **Costa Rica** have some general guidelines provided by the ministry of science and technology.

68. Overall, respondents reported that accountabilities were well-defined for digital security in health, with clarity for alignment and co-ordination across organisations. Many of these groups were also co-ordinating across borders. This alignment supports cooperation within and across sectors and within and across countries (see section 3.2.4).

3.2.3. Human Rights and Fundamental Values

69. The Lancet Report on *Governing Health Futures* articulated that digital transformation should be considered a determinant of health (The Lancet Digital Health, 2021[17]). The report encouraged governance that creates trust in digital health by enfranchising patients and vulnerable groups, ensuring health and digital rights, and regulating powerful players in the digital health ecosystem.

70. Trust and enfranchisement are built on common language, active engagement, and transparent communication. Digital literacy is not innate and safe digital behaviour is not intuitive. Digital literacy helps build trust in the use of digital tools through understanding the purpose of the technology and the safeguards in place to protect their personal health information. Public participation identifies the most important digital security risk mitigations and the communications necessary to build and sustain trust, including in case of a security breach. Such public engagements are essential to understand societal values for the use and protection of health data which inform policies for privacy and security. Finally, transparent communication with impacted parties in case of a security breach helps to foster trust.

71. Respondents were asked to share their approach to public participation, digital literacy, and communications. (Table 3.4)

Table 3.4. Public Involvement and Digital Literacy

	Public participation approach	Digital literacy programs for the public	Who oversees the digital literacy program?	Communication plans for security breach
Australia	Yes	Yes	The Australian Digital Health Agency have training modules and information	Yes
Belgium	n.r.	Yes	n.r.	No
Canada	Yes	Yes	Canadas Centre for Cyber Security	Yes
Costa Rica	n.a.	No	n.r.	No
Croatia	Yes	Not by health services	National Security Council have education programs and workshops for public sector officials	Yes
Czechia	No*	No	n.a.	Yes
France	n.r.	Yes	Online platform	n.a.
Germany				
Greece	Yes	Yes	Ministry of Digital Governance	Yes
Ireland	Yes	Yes	National Cyber Security Centre	Yes
Israel	Yes	Yes	Survey digital literacy	Yes

Italy	Yes	Yes	Plan for increased digital literacy among students and teachers, online learning modules, non-profit organisations working on digital literacy, promoting digital culture thought awareness of cyber risk.	Yes
Japan	Yes	Yes	n.r.	Yes
Korea	Yes	Yes	Training and manuals	Yes
Lithuania	No	No		Yes
Luxembourg	Yes	Not by health services	Programs run by non-health organisations	Yes
Netherlands	Yes	No	n.r	No
Norway	Yes	Not by health services	The Norwegian Center for Information Security provides information and support	Yes
Portugal	Yes	Yes	Portuguese Safe Internet Centre promote safe and responsible internet and technology use	Yes
Slovak Republic	Yes	Yes	National Cybersecurity Center raise awareness	Yes
Slovenia	Partly	Not by health services	n.r.	Yes
Spain	Yes	Not by Health services	Spanish National Cybersecurity Institute (INCIBE) and CCN-CERT.	Yes
Switzerland	Yes	Yes	National Cyber Security Centre	No
United Kingdom	Yes	n.r.	n.r.	Yes
United States	Yes	Yes	n.r	Yes

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., * is currently being implemented
Source: OECD 2023 Digital Health Security questionnaire.

72. Eighteen respondents explicitly reported having public participation activities to understand public requirements and expectations for digital security. **Australia** consults the public before major initiatives; **Croatia** publishes public announcements through multiple channels; **Ireland** has several patient body engagement forums for which digital security is covered; **Israel** informs the public about risks; and in **Canada**, **Italy, Japan, Korea, Lithuania, Luxembourg, Netherlands, Portugal, The Slovak Republic, Slovenia, Spain, Switzerland, Norway, and the United Kingdom** have public requirements for digital security are embedded in legal or organisational requirements.

73. When promoting digital literacy, countries differ in whether and how this is done. Fourteen respondents indicate that their country has some form of digital literacy programme by health organisations aimed at the public. **France** has a program embedded within their public health data portal – *MonEspaceSanté*. Other countries reported efforts to improve digital literacy through online education modules (**Australia, Canada, Korea, Italy and Portugal**), open publication of digital controls and terminology (**Croatia, Slovak Republic, Switzerland and Norway**), developing a handbook (**Greece**), surveys on digital literacy (**Israel**), courses for students and public service officials (**Canada, Croatia** and **Italy**), and public literacy campaigns (**Belgium, Italy, Portugal** and **Switzerland**) that support transparency and raise awareness.

74. Overall, respondents are actively involving the public in the design, implementation, and evolution of their digital security in health programs, including active efforts to improve digital literacy. Almost all countries had a transparent process for communicating cyber incidents with the public.

3.2.4. Co-Operation

75. With digital transformation, health systems are becoming more interconnected. As demonstrated by the WannaCry attack in 2017 (see Table 3.1), an attack on one organisation can quickly spread to

others. While cyberattacks are directed at specific organisations, strong collaboration and cooperation can help organisations that have not yet been impacted implement appropriate protections.

76. Respondents were asked to share their approach to co-operation. Aspects of co-operation were also covered in the responses to section 3.2.2 above. (Table 3.5)

Table 3.5. Communication within and across organisations processing health data

	In the organisation, is there a program in place to communicate potential security threats internally?	Does the security program include communications across organisations?
Australia	Yes	Yes
Belgium	Yes	Yes
Canada	Yes	Yes
Costa Rica	Yes	Yes
Croatia	Yes	Yes
Czechia	Yes	Yes
France	n.r.	n.r.
Germany	n.r.	n.r.
Greece	Yes	Yes
Ireland	Yes	Yes
Israel	Yes	Yes
Italy	Yes	Yes
Japan	Yes	Yes
Korea	Yes	Yes
Lithuania	Yes	Yes
Luxembourg	Yes	Yes
Netherlands	Yes	Yes
Norway	Yes	Yes
Portugal	Yes	Yes
Slovak Republic	Yes	No
Slovenia	Yes	Yes
Spain	Yes	Yes
Switzerland	Yes	Yes
The United Kingdom	Yes	Yes
The United States	Yes	Yes

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented
Source: OECD 2023 Digital Health Security questionnaire.

77. All respondents reported the existence of a plan for communication internal to the impacted organisation in the event of a threat. All countries except for **Czechia** reported communication of cyber threats across organisations.

78. Overall, with clear accountabilities for coordination (3.2.2 above) and the findings above, respondents have communications in place to cooperate during a cyberevent. Across these areas there is also indication of cross-border collaboration led by the designated coordination function.

3.2.5. Strategy and Governance

79. Governance manages the risk of digital security in health while aligned to the overall strategy of health systems. Significant aspects of governance include designating accountability (see 3.2.2), defining the amount of acceptable risk for the organisation, and ensuring there are sufficient resources to manage digital security risk within those constraints.

80. Strong strategy and governance bring alignment across organisations which helps to mitigate the likelihood and impact of a threat. This approach is being adopted across industries for common technology services such as cloud (Deloitte, 2023[18]).

81. Respondents were asked to share their approach to strategy and governance, including the financing of digital security risk management. Table 3.2 includes some cross-industry benchmarks on funding for digital security. (See Table 3.6)

Table 3.6. Management and Accountability in Organisations

	Managing digital security risk is part of an overall approach to risk management	The risk management approach is aligned	Distinct budget for digital security * Of those reporting, ranging from 8-15%
Australia	Yes	Yes	Yes
Belgium	Yes	No	Partly
Canada	Yes	Yes	Yes
Costa Rica	No	Yes	No
Croatia	Yes	Yes	No
Czechia	No	Yes	No
France			
Germany			
Greece	Yes	Yes	Yes
Ireland	Yes	Yes	Yes
Israel	Yes	Yes	Yes
Italy	Yes	No	n.r.
Japan	n.r.	n.r.	n.r.
Korea	Yes	Yes	Yes
Lithuania	Partly	No	Yes
Luxembourg	Yes	No	Yes
Netherlands	Yes	No	Yes
Norway	Yes	Partly	Partly
Portugal	Yes	Yes	Yes
Slovak Republic	Yes	Yes	Yes
Slovenia	Yes	No	No
Spain	Yes	Yes	No
Switzerland	Partly*	Yes	No
The United Kingdom	No	No	Yes
The United States	n.a.	n.a.	n.a.

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented, ***Switzerland** situation varies across systems and organisations. For example, their National Electronic Patient Record have mandatory responsibilities of their systems while the system for vaccination and contract tracing during COVID-19 did not.
Source: OECD 2023 Digital Health Security questionnaire.

82. In most countries, the responsibility for digital security risk management is within individual organisations responsible for their technologies. Thirteen countries reported that digital security risk management was explicitly aligned across organisations.

83. In **Czechia** cyber security is managed separately from risk management. Several countries identified that digital security risk management is managed, monitored, and regularly assessed by the central system manager identified in section 3.2.2. In **Switzerland** the situation varies across systems and organisations. For example, their National Electronic Patient Record have mandatory responsibilities of their systems while the system for vaccination and contract tracing during COVID-19 currently do not.

Similarly, in the **United Kingdom** each organisation is responsible for their own risk, thus variation remains. Also, within the **United Kingdom** countries there are variations, as **Scotland** has developed the Public Sector Cyber Resilience Framework (PSCRF) which aligns public sector organisation risk management. **Belgium** is currently developing a standardised approach across the organisations.

84. Twelve countries (**Australia, Canada, Greece, Ireland, Israel, Korea, Lithuania, Luxembourg, Netherlands**, **Portugal, Slovak Republic, and the United Kingdom**) reported an explicit budget for digital security in their technology budgets. Of their technology budget, the budget for digital security ranged from 8 to 15%, for those countries that explicitly reported a numerical value. Other countries (**Croatia, Czechia,** and **Slovak Republic)** reported accessing EU funds to finance individual security projects with clear objectives. Lastly, **Belgium**, did do not have a distinct budget for digital security in their Covid services, but have distinct budgets for other health data projects.

85. Overall, there is a mixed response to how digital security risk management is integrated across health systems, although the majority report alignment with the designated coordination function from section 3.2.2. As such, digital security risk management is centrally coordinated and locally implemented. Further, where direct investment has been identified, it is approximately 10% of IT budgets which is aligned with amount from other industries (see Table 3.2).

Box 3.2. Financial industry technology investments in digital security

86. Significant expense is required to prevent cyberattacks and minimise their impact. The costs of digital security in health are determined by organisations based on their current digital footprint. Costs involve investments to drive a culture of digital security as well as technologies to detect, prevent, respond, and remediate cyberthreats. Digital security risk management should be addressed as a business risk with a significant IT investment.

87. As a benchmark, the financial industry spent on average 10.9% of their IT budgets on cybersecurity in 2020 (SenseOn, 2022[19]).

88. By contrast, recent reports from the US health sector estimate that 5% of IT budgets were allocated to cybersecurity in hospitals and that 80% of those hospitals suffered a successful cyberattack (Garrity, 2019[20]).

89. Increasing investment for digital security is a modest investment to prevent the potential costs involved in discontinuity of health services and the negative impacts they cause for the public, providers, and health systems.

3.2.6. Risk assessment and treatment

90. Digital security risks and mitigation plans should be periodically assessed to ensure that the risk mitigation measures are in place and new risks are being addressed. This assessment can also evaluate the effectiveness of the digital security program to ensure its ongoing relevance and priority for decision-makers. This review can include areas such as ‘number of employees receiving security training’, ‘cost of security program’, and ‘impact of security breaches’. These processes may also provide perspective on the state of digital security risks and emerging methods for detection and prevention (see section 3.2.9on Innovation).

91. Respondents were asked to share their approach to ongoing monitoring and evaluation of the digital security program, which includes periodic risk assessment and treatment. (Table 3.7)

Table 3.7. Monitoring and evaluation of digital security program

	There is regular reporting of the performance of the digital security program	Frequency	Method
Australia	Yes	Confidential	Confidential
Belgium	Yes	Monthly	Reports
Canada	Yes	Annually	Reporting (w/other agencies)
Costa Rica	No	-	-
Croatia	No	Ad-hoc	Reports
Czechia	Yes	Annually	Reports
France			
Germany			
Greece	Yes	Annually	Reports
Ireland	Yes	Monthly	Program Progress Reports
Israel	n.r.	-	-
Italy	Yes	Continuously	n.r.
Japan	Yes	Continuously	n.a.
Korea	Yes	Monthly	Reports
Lithuania	Yes	Annually	Reports
Luxembourg	Partly	Varies	
Netherlands	Yes	Monthly	Failure Mode Effect Analysis (FMEA)
Norway	Partly	Monthly	Reports
Portugal	n.r.	n.r.	n.r.
Slovak Republic	No	n.r.	Reports
Slovenia	Yes	Daily	Reports
Spain	Yes	Annual	Reports
Switzerland	Yes	n.r.	Security impact assessment
The United Kingdom	Yes	Annual	Reports
The United States	Yes	No prescribed frequency	n.a.

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented, ***can be variation between state government and private health organisations
Source: OECD 2023 Digital Health Security questionnaire.

92. Sixteen responding countries have regular reporting of the digital security programme by the responsible organisation. The frequency of these reports varies as six countries report annually (**Canada**, **Czechia**, **Greece**, **Lithuania**, **Spain, and the United Kingdom**), four countries have monthly (**Ireland**, **Korea**, **Netherlands** and **Norway**), three countries have continuous (**Italy, Japan,** and **Slovenia**), two indicated reporting was ad-hoc (**Croatia and the United States**) and one reported security assessment by a pool of expert before major changes (**Switzerland**).

93. **Norway** indicated that its main processor, NHN, is mandated to report monthly on security-related issues whereas there is no mandated frequency for other organisations. **Switzerland**, clarify that no program is present at the national level and organisations have local reporting at a variety of frequencies. **Switzerland's** COVID system will introduce digital security reporting this year. In **Luxembourg**, reporting is dependent on the organisation.

94. Overall, countries have a mixed approach to reporting and evaluation of the effectiveness of digital security in health with a variety of frequencies and accountabilities for evaluation and reporting.

3.2.7. Security measures

95. Alongside strategic digital security risk management, it is also important to have strong practices for operational security measures to monitor for new threats and implement security patches when available.

96. Pro-active security measures could include actions in both business and technology teams; however, most responses included measures that focussed on technology. (Table 3.8)

Table 3.8. Risk assessment and treatment

	The organisation monitoring the security	Frequency	There is a pro-active program for security measures	Pro-active measures
Australia	Yes	Continuous monitoring***	Yes	Patching, multi-factor authentication, audit logs, firewalls, regular anti-virus scanning, system monitoring
Belgium	Yes	Continuous monitoring	Yes	Patching
Canada	Yes	Continuously monitoring	Yes	Patching, vulnerability management, continuous security verification activities.
Costa Rica	Partly	Applied against demand	Yes	
Croatia	Yes	Periodic (usually annual)	Yes	Patching, antivirus and anti-spam software, IT equipment's updates
Czechia	Yes	Continuous monitoring	Yes	Patching
France				
Germany				
Greece	Yes	Annually and in major changes	Yes	Patching, antivirus management, management of access, monitoring
Ireland	Yes	Annually	Yes	Legacy renewal, migration to Cloud technology, and active threat & vulnerability management program
Israel	Yes	Continuously	Yes	Risk assessment evaluation
Italy	Yes	Periodically, dependent of type of threat, level of risk and sensitivity of the data.	Yes	Patching, updates, reviews
Japan	Yes	Continuously monitoring	n.r	n.a.
Korea	Yes	Continuously monitoring and audits once a year	Yes	Patching and monthly checking of computers
Lithuania	Yes	Report once a month and continuous scans	Yes	Recommended updates once a week
Luxembourg	Yes	Once a year and real-time monitoring	Yes	n.r.
Netherlands	Yes	Continuous monitoring	Yes	Penetration tests and patching
Norway	Yes	vulnerability assessment weekly basis, central system reports every six months	Yes	Patching
Portugal	Yes	Frequency dependent on organisation and level of risk	Yes	Proactive vulnerability scanning
Slovak Republic	Yes	SIEM	Yes	Patching and vulnerability scanning
Slovenia	Yes	Continuously monitoring	Yes	Patching
Spain	Yes	Annual audits	Yes	Patching
Switzerland	Yes	Required before major changes	Yes	n.r.
The United Kingdom	Yes	Continuously monitoring	n.r.	n.r.
The United States	Yes	No frequency prescribed	Yes	Patching

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented, ***can be variation between state government and private health organisations
Source: OECD 2023 Digital Health Security questionnaire.

97. All but one country reported that organisations carry out periodic reviews of their technology systems. Continuous monitoring of the systems is conducted in several countries (**Australia, Canada, Czechia, Japan, Korea, Luxembourg, Netherlands, Slovenia, and the United Kingdom).** In addition, several countries (**Belgium**, **Croatia, Greece, Ireland, Korea, Luxembourg, Norway, Spain Switzerland**) report that audits are carried out on an annual or monthly basis. **Costa Rica** and **The United States,** who do not require its organisations to monitor their systems on a regular basis, report that it addresses security on an ad hoc basis. **Switzerland** do not have a formal process, rather they review their technology systems against demand or in the event of changes to the infrastructure.

98. Almost all countries reported at least one type of proactive program to prevent security breaches. Those programs included system patching and vulnerability (e.g., anti-virus) scanning of technical equipment. Notably, **Korea** requires monthly computer scans to be performed by individuals, providing both security protections and improvements to security awareness.

99. Overall, countries have continuous monitoring in place to detect cyberthreats. Further, proactive protections are in place such as vulnerability scanning and actively applying security patches when available.

3.2.8. Resilience, Preparedness and Continuity

100. The first seven principles focussed on strong cultural awareness of the importance of digital security, clear accountability, cooperation across organisations, and a proactive approach to risk management. It is also important for organisations to have processes in place to be able to be prepared to respond in case of a cyberattack. Remediation to a cyberevent could take several months. This implies that a robust approach to being prepared is helpful for resilience to minimise the impact of a shock.

101. Respondents were asked to share their approach to be prepared in case of an attack. (Table 3.9)

Table 3.9. Resilience, Preparedness, and Continuity

	Clear accountabilities and escalations plan	Type of plan	Periodic security intrusion test	Frequency
Australia	Yes	Business continuity and disaster recovery plans. No paper-based plans, individual clinics must access relevant data though local systems	Yes	Confidential
Belgium	Yes	Continuity plans	Partly	Non-periodic
Canada	Yes	IT continuity plans, business recovery and disaster recovery	Yes	Periodic reviews
Costa Rica	Yes	Paper based	Yes	Non-periodic
Croatia	Yes	Paper based	Yes	Ahead of platform launching
Czechia	Yes	Business impact assessment, business continuity management plans, and theoretical paper based	Yes	Test major changes
France				
Germany				
Greece	Yes	Disaster recovery plans	Yes	In event of changes to infrastructure and ad-hoc

Ireland	Yes	Cyber Incident Response 'playbook'	Yes	In the event of changes to infrastructure and ad-hoc
Israel	Yes	Disaster recovery plans and business continuity plans	Yes	Annually
Italy	Yes	Disaster recovery plans and business continuity plan	Yes	Quarterly or semi annual
Japan	Yes	n.r.	Yes	Ad-hoc
Korea	Yes	Disaster recovery plan, backup and dissipate data	Yes	Annually
Lithuania	Yes	Digital format transferred with delay (worst case scenario)	Yes	Annually
Luxembourg	Yes	Each hospital has own plans, for COVID system is there a pandemic continuity plan, DRP plan and on call service.	Varies	Annually (eSante)
Netherlands	Yes	Business continuity plans. Third-party storage of logs and backup data for recovery.	Yes	In the event of changes to infrastructure and ad-hoc
Norway	Yes	Business Continuity, disaster recovery plan and escalation procedures	Yes	Non-regular
Portugal	Yes	Business Continuity and disaster recovery plan, some cases there are paper-based plan	Yes	non-regular
Slovak Republic	Yes	Business continuity and disaster recovery plans	Yes	n.r.
Slovenia	Yes	Business Continuity and disaster recovery plans	Yes	Annually
Spain	Yes	Technology continuity and disaster recovery plans	Yes	n.r.
Switzerland	Yes	Business continuity plans	Yes	Non-regular
United Kingdom	Yes	Business continuity and disaster recovery plans	Yes	Non-regular
United States	n.a	Contingency plans and disaster recovery plans	Yes	Non-regular

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented, ***can be variation between state government and private health organisations
Source: OECD 2023 Digital Health Security questionnaire.

102. As shown in table 3.9 all respondents have plans in place for backup and recovery including in the case of cyber security incidents. Thirteen countries (in **Australia, Canada, Israel, Italy, Korea, Lithuania, Luxembourg, Netherlands, Slovak Republic, Slovenia, Spain, the United Kingdom** and **The United States**) explicitly mention a disaster recovery plan. Business continuity plans are mentioned by **Czechia, Netherlands**, the **Slovak Republic, Slovenia,** and **Switzerland**. **Belgium** is currently improving their protocol for the event of a cyber-attack; this includes reviewing their critical systems and operational needs in the event of a prolonged disruptive incident. **Ireland** will introduce proactive and continuous assessments of vulnerabilities in their digital environment.

103. Annual testing to simulate a cyberattack to test their ability to respond are carried out in six countries (**Israel, Korea, Lithuania, Italy, Luxembourg,** and **Slovenia**). Six countries, on the other hand, test their system on a non-regular basis; these are **Belgium**, **Costa Rica**, **Norway**, **Portugal**, **Switzerland**, and **the United Kingdom**. Whereas testing systems ahead of major changes is conducted in **Croatia** and **Czechia**. Lastly, **Canada** also tests their systems, but don't indicate interval of the tests.

104. Overall, countries have backup and recovery plans in place for technology in health organisations. Some also have established an integrated approach across business and technology. Countries are performing periodic penetration tests in place to detect potential vulnerabilities to cyberthreats.

3.2.9. Innovation

105. Digital security is an arms race with both attackers and defenders advancing their capabilities in parallel (Samtani, 2022[21]). Further, with the continued growth of digitalisation in the health sector, organisations without a structured approach to digital security are at risk of being caught in the crossfire. While the previous sections have focussed on digital security protections for the current state, it is necessary to continually innovate and improve.

106. Respondents were asked to share innovations in digital security that were in process of investigation or implementation. Below the table is a brief description of selected innovations. (Table 3.10)

Table 3.10. Innovations being explored or implemented.

	Leading and emerging methods	What are examples of innovations begin explored / implemented?
Australia	Yes	Identity management, multifactor authentication, data encryption
Belgium	Yes	Invest in new and emerging security technologies
Canada	Yes	Invest in new and emerging security technologies
Costa Rica	No	
Croatia	Yes	Mandatory VPN, smart cards for health professionals, state-owned PKI infrastructure, authentication, authorisation, role-based access, audit logging, non-repudiation digital signaling, enforced encryption.
Czechia	Yes	Identity management, multifactor identification, encryption for data in rest and motion, synthetic data, role-based access, managed network, monitoring, security log correlation, geographical redundance
France		
Germany		
Greece	Yes	Encryption data in motion and rest, role base access, and plan for cloud-based integration
Ireland	Yes	Digital security framed on six key principles: ICT & Cyber governance, Compliance, Security Operations, Foundational Technology, Threat & Vulnerability Management, IT service & asset management
Israel	Yes	Multi-factor identification, encryption for data in rest and motion, synthetic data, role-based access, cloud technology
Italy	Yes	Multi-factor authentication, Encryption, backup and disaster recovery, Firewalls, Intrusion Detection, Preventive systems, regular security audits
Japan		n.r
Korea	Yes	Public authentication, simple authentication, OTP, apply blockchain encryption (COOV system) and cloud-based technology
Lithuania	Yes	Multi Factor authentication, Role based access
Luxembourg	Yes	Identity management, multi-factor authentication, Encryption for data at rest and in motion, synthetic data, role-based access, cloud technologies
Netherlands	Yes	Use of cloud technologies, OpenKAT bi-temporal graph database for continuous compliance testing
Norway	Yes	Multi-factor authentication, Zero-trust, micro-segmentation, endpoint security monitoring, encryption
Portugal	no	
Slovak Republic	no	
Slovenia	Yes	Identity management, multi-factor authentication, encryption of data in motion
Spain	Yes	Multiple methods
Switzerland	n.a.	
The United Kingdom	Yes	Secure backup data
The United States		n.r

Note: n.r. not reported, n.a. not applicable, awareness is using intranet to inform about specific security threats and news., ** is currently being implemented, ***can be variation between state government and private health organisations
Source: OECD 2023 Digital Health Security questionnaire.

107. Overall, most countries are implementing leading practices in digital security, and several are exploring emerging tools and capabilities. Some examples of these are described below and includes some other examples from a review of literature. (Table 3.11)

Table 3.11. Description of leading practices and emerging tools in digital security

Leading practice / emerging tool	Description
Role-based access / identity management	Data access control mechanisms refers to technical and organisational measures that enable safe and secure access to data by approved users. Role-based ensures that access is appropriate for the role of the individual. Identity management ensures that users are authenticated against their access periodically.
Multifactor authentication	The use of multiple channels to authenticate users prior to enable access to data and systems.
Zero-trust policy	In this security system design, all entities—inside and outside the organisation's computer network—are not trusted by default and must prove their trustworthiness. Zero-trust shifts the focus of cyberdefense away from the static perimeters around physical networks and toward users, assets, and resources, thus mitigating the risk from decentralized data.
Data encryption	Encryption is the transformation of data using cryptography to produce unintelligible data to ensure its confidentiality. Data may be encrypted at rest (e.g., when stored in databases), in motion (e.g., when moving between databases). Some are leveraging Blockchain to support encryption.
Synthetic data	An approach to confidentiality where instead of disseminating real data, synthetic data that have been generated from one or more population models are released.
Elastic log monitoring	Elastic log monitoring allows companies to pull log data from anywhere in the organisation into a unique location and then to search, analyze, and visualize it in real time to identify unusual data access patterns.
Homomorphic encryption	This method allows users to work with encrypted data without first decrypting it, thus giving third parties and other collaborators safe access to large data sets.
Secure software development	Cybersecurity embedded in the design of software from inception. Security and technology risk teams should engage with developers throughout each stage of development. Security teams should also adopt more systematic approaches to problems, including agile and Kanban.

Source: (Mckinsey and Company, 2023[2]; OECD, 1997[22]; OECD, 2021[23])

3.3. Leading practices for digital security in health

108. Digital security is increasing in its importance in health to match the growth of digitalisation. Most OECD countries are taking action to strengthen their approach to digital security, although there is variation in the breadth and frequency of practices.

109. The table below findings related to key components of a robust digital security risk management program. This includes proposed leading practices and countries aligned with that leading practice. (Table 3.12)

Table 3.12. Leading practices in Respondents for Digital Security in Health

Principle	Question	**Leading Practice**	**# Of Respondents (/25)**
Digital Security Culture: Awareness, skills, and empowerment	Is there a program for security training within all organisations?	Yes	All but Italy (who is currently implementing it)
	Is digital security training required at least annually?	Yes	Australia, Greece, Ireland, Israel, Japan, Korea, Luxembourg, Netherlands, Norway, The Slovak Republic, Slovenia, Spain, The United Kingdom
	Is there a common curriculum across organisations?	Yes	Australia, Czechia, France, Greece, Ireland, Ireland, Israel, Korea, Norway, Portugal, Spain, The United Kingdom

	Are there pro-active measures to foster digital security culture?	Yes	Australia, Greece, Canada, Costa Rica, Croatia, Greece, Japan, Ireland Israel, Italy, Korea, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Slovenia, Spain, The United Kingdom, The United States.
	Are all 'leading practices' for digital security culture in place? (Phishing simulations, awareness campaigns)	Phishing Awareness	Australia, Canada, Ireland, Israel
Responsibility and Liability	Are there defined key roles and responsibilities for digital security within organisations?	Yes	Australia, Belgium, Canada, Croatia, Czechia, Greece, Japan, Ireland, Israel, Italy, Korea, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Slovenia, Spain, Switzerland, The United Kingdom, The United States
	Is there a national digital security in health program that aligns peer organisations?	Yes	Australia, Belgium, Croatia, Czechia, Greece, Japan, Ireland, Israel, Italy, Korea, Lithuania, Luxembourg, Norway, Portugal, Spain, Switzerland, The United Kingdom, The United States
	Is there a defined accountable organisation to coordinate actions?	Yes	Australia, Canada, Croatia, Czechia, Greece, Japan, Ireland, Israel, Italy, Korea, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovenia, Spain, Switzerland, The United Kingdom, The United States
	Is there a national digital security in health program that is aligned with a national cross-industry digital security program?	Yes	Australia, Canada, Costa Rica, Croatia, Czech, Greece, Japan, Ireland, Israel, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovenia, Spain, Switzerland, The United Kingdom, The United States.
		Both digital and health align digital security in health	Korea, Norway, Portugal, Slovenia, the United Kingdom
Human rights and fundamental values	Is there a public participation approach in understanding public requirements for digital security?	Yes	Australia, Canada, Croatia, Greece, Israel, Italy, Japan, Korea, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Spain, The United Kingdom, The United States.
	Is there a digital literacy program for the public that includes digital security protections?	Yes	Australia, Belgium, Canada, France, Greece, Israel, Italy, Japan, Korea, Portugal, Slovak Republic, Switzerland, Spain, The United States
	Are there standard communication plans in the case of a security breach that includes the public when appropriate?	Yes	Australia, Canada, Croatia, Czechia, Greece, Ireland, Israel, Italy, Japan, Korea, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Slovenia, Spain, The United Kingdom, The United States.
Co-operation	Is there a program in place to communicate potential threats within organisations?	Yes	All respondents.
	Is there a program in place to communicate potential threats across peer organisations?	Yes	All respondents.
Strategy and Governance	Is managing digital security risk in health is part of an overall approach to risk management?	Yes	Australia, Belgium, Canada, Croatia, Greece, Ireland, Israel, Italy, Korea, Luxembourg, Netherlands, Norway,

			Portugal, Slovak Republic, Slovenia, Spain.
	Is risk management approach is aligned across organisations?	Yes	Australia, Canada, Costa Rica, Croatia, Czechia, Greece, Ireland, Israel, Japan, Korea, Portugal, Slovak Republic, Spain, Switzerland.
	Is there a distinct budget for digital security?	Yes	Australia, Canada, Greece, Ireland, Israel, Korea, Lithuania, Luxembourg, Netherlands, Portugal, Slovak Republic, The United Kingdom.
	Is the budget > 10% (comparable to Financial Industry)?	>10%	Israel, Korea, Lithuania, Netherlands.
Security Measures	Is the organisation accountable for the system and monitoring security?	Yes	Australia, Belgium, Canada, Croatia, Czechia, Greece, Ireland, Israel, Italy, Korea, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Slovenia, Spain, Switzerland, The United Kingdom, The United States.
	Is the frequency of security monitoring procedures continuous?	Continuous	Italy, Netherlands
Risk assessment and treatment	There is regular reporting of the performance of the digital security program?	Yes	Australia, Belgium, Canada, Czechia, Greece, Ireland, Italy, Japan, Korea, Lithuania, Netherlands, Slovenia, Spain, The United Kingdom, The United States.
	Is the frequency of the digital security program evaluated and reported at least quarterly	Yes	Australia, Belgium, Canada, Czechia, Israel, Japan, Korea, Lithuania, Luxembourg, Netherlands, Slovenia, The United Kingdom
Innovation	Are role-based access, identify management, multi-factor authentication, and data encryption (at rest and in motion)	Yes	Australia, Croatia, Czechia, Israel, Italy, Korea, Luxembourg, Norway, Slovenia.
Resilience, preparedness & continuity	Are there clear accountabilities in the case of a security breach?	Yes	All respondents
	Are there business continuity and disaster recovery plans in place?	Yes	Australia, Canada, Czechia, Israel, Italy, Netherlands, Portugal, Slovak Republic, Slovenia, Spain, The United Kingdom, The United States
	Are there periodic security penetration tests?	Yes	Australia, Canada, Costa Rica, Croatia, Czechia, Greece, Ireland, Israel, Italy, Japan, Korea, Lithuania, Netherlands, Norway, Portugal, Slovak Republic, Slovenia, Spain, Switzerland, The United Kingdom.

110. The following table summarises the alignment between countries and proposed leading practices by each digital security principle. Green represents 100% alignment with leading practice across all questions in the table above. Yellow is less than 100% alignment. Grey represents where answers were incomplete, deemed confidential, or a single answer didn't apply because of diverse requirements and other factors. Figure 3.1 is grouped by whether countries had a strategy for digital security in health (aligned with an overall national strategy), whether there is only a national strategy for digital security, or whether there was not an indicated national strategy.

Figure 3.1. Summary of alignment of countries to leading practices by principle

		Digital security culture	Responsibility and liability	Human rights and fundamental values	Co-Operation	Strategy and Governance	Security Measures	Risk assessment and treatment	Innovations	Resilience, Preparedness and Continuity
		Digital Security Principles								
Digital Security Strategy specific to Health (**bolded** countries identified alignment with a national digital health strategy)	**Australia**	G	G	G	G	G	G	I	G	G
	Canada	Y	Y	G	G	Y	G	Y	G	G
	Czechia	Y	G	Y	G	Y	G	Y	G	G
	France	I	I	I	I	I	I	I	I	I
	Germany	I	I	I	I	I	I	I	I	I
	Ireland	G	G	G	G	G	G	G	G	G
	Israel	G	G	G	G	Y	G	Y	G	G
	Netherlands	Y	Y	Y	G	Y	G	G	Y	G
	Norway	Y	Y	G	G	Y	G	Y	G	Y
	United Kingdom	G	G	Y	G	Y	Y	Y	Y	G
	United States	Y	G	Y	G	Y	G	G	G	Y
National Digital Security Strategy	Costa Rica	Y	Y	Y	G	Y	Y	Y	Y	Y
	Croatia	Y	G	G	G	Y	G	Y	G	Y
	Italy	Y	G	G	G	Y	G	G	G	G
	Japan	Y	G	G	G	I	Y	Y	I	Y
	Korea	G	G	G	G	G	G	G	G	G
	Lithuania	Y	Y	Y	G	Y	G	Y	G	G
	Portugal	Y	G	G	G	Y	G	Y	Y	Y
	Slovenia	Y	Y	Y	G	Y	G	G	G	G
	Spain	Y	G	G	G	Y	G	Y	Y	G
	Switzerland	Y	G	Y	G	Y	Y	Y	Y	G
No reported Digital Security Strategy	Belgium	Y	Y	Y	G	Y	G	G	G	Y
	Greece	Y	Y	G	G	Y	G	Y	G	G
	Luxembourg	Y	Y	G	G	Y	G	Y	G	Y
	Slovak Republic	Y	Y	G	Y	Y	G	Y	Y	G

Source: Questionnaires for fast-track paper on digital security risk management in health

111. Overall, 75% of responses are aligned with the proposed leading practice. Respondents that had a specific strategy for digital security in health (that was aligned with a national strategy) had a higher alignment with leading practice in 6.1 of the 9 principle areas. Respondents with a national digital security strategy were aligned with leading practice on average in 4.7 of the 9 principle areas. Countries without a digital security in health strategy were aligned in 4.5 of the 9 principle areas.

112. Digital security culture is somewhat in place across all respondents. Countries that had a specific digital security strategy for health were more aligned with leading practices. The major difference is having pro-active measures in place, such as raising awareness through education campaigns or phishing simulations. Specifically, **Australia, Ireland, Israel**, **Korea**, and the **United Kingdom** are best aligned with the leading practices.

113. Clarifying responsibility and liability is stronger in countries that have a specific strategy for digital security in health or align with a national digital health strategy. In some countries (**Korea**, **Norway**, **Portugal**, **Slovenia**, and the **United Kingdom**) co-ordination are supervised by multiple entities that have responsibility for health and broader aspects of digitalisation. **Australia, Croatia, Czechia, Ireland, Israel, Italy, Japan**, **Korea**, **Norway**, **Portugal, Spain, Switzerland,** the **United States**, and the **United Kingdom** are best aligned with the leading practices.

114. There are a variety of approaches for human rights and fundamental values. Leading practice encourages active engagement and transparent communication with the public along with improvements in digital literacy. Responding countries best aligned with human rights and fundamental values are **Australia**, **Canada**, **Croatia, Czechia, Greece, Ireland, Israel**, **Italy, Japan**, **Korea**, **Norway, Portugal**, **Spain,** and **the United Kingdom**.

115. Almost all respondents reported good cooperation within organisations and with peer organisations.

116. For strategy and governance, questions were asked about the alignment of digital security to the overall strategy of health systems. Fourteen countries reported digital security management being a part of the overall approach to risk management. Only half of the respondents reported distinct budgets for digital security and only four (**Australia, Korea, Lithuania, and the Netherlands)** reported allocation to digital security in line with other industries.

117. Security measures, such as applying patches and screening for viruses, are critical to the overall approach to digital security as noted in the WannaCry attack (Table 3.1). **More than two thirds** of respondents had proactive programs which perform these functions.

118. Digital security risks should be periodically assessed and mitigated. Among the respondents, 11 out of twenty-five have regular reporting of the performance of the digital security program; however, the interval of reporting varies from daily, monthly, annually and ad-hoc. Leading practice would be to review at least quarterly as is seen in **Belgium, Italy, Korea,** and **Slovenia**.

119. For innovation, there are many leading and emerging methods in digital security that are reported by the responding countries. Leading practices are to investigate (and ideally adopt) role-based access, identify management, multi-factor authentication, and data encryption for data at rest and in motion. **More than half** of respondents are examining these areas and implementing those practices as appropriate.

120. For resilience, preparedness and continuity, all respondents had escalation plans for cyberattacks, many of which both mentioned business continuity plans and disaster recovery plans. There is variation in country approaches to penetration tests to simulate a security breach ensure that processes are ready. **More than half** of respondents were performing some form of penetration testing.

121. Overall, from this limited survey, it appears that **Ireland** and **Korea** are aligned with all leading practices for digital security in health. **Australia**, **Canada**, **Israel,** and **Italy** also responded with strong alignment. The analysis shows some key priority areas for government action to align with the OECD Digital Security Risk Management Framework and cooperate in areas of mutual benefit. These include:

1. improving digital security culture where only 5 of 25 countries were aligned with leading practice. **Israel** is promoting a culture of digital security through initial and refresher training programs for all employees as well as periodic phishing and cyberattack simulations;

2. strengthening strategy and governance where only 3 of 25 countries were aligned with leading practice. In **Australia,** managing digital security risk in health is part of an overall approach to risk management and at least 10% of IT budgets are allocated to digital security (which is in line with other industries); and
3. embedding risk assessment and treatment where only 7 of 25 countries were aligned with leading practice. For example, countries could monitor and report the effectiveness of the digital security program at least quarterly to ensure that digital security risks are always top of mind.

122. It is notable that some areas for improvement to mitigate digital security risks are relatively low-cost (such as training staff and monitoring programs) when compared to extensive interventions such as advanced security solutions, security audits and penetration testing, amongst others. It is estimated that 90% of digital security challenges start with phishing. Hence these low-cost activities could also be among the most effective.

4. Moving forward to strengthen digital security

123. COVID-19 was a significant disruption in many countries that proliferated new systems, new connections, and new uses of health data and digital tools, including COVID-19 testing, contact tracing, vaccination deployment, and virtual care. This required the ability to upscale legacy or build new systems at high speed in hospitals, public health units, and primary care. All these new investments had some level of digital security risk.

124. Digital security risk in health has been a priority at an international level, including:

- the G20 Minister Declaration in 2020 ("To strengthen trust in digital health solutions, consistent with applicable law and regulation, we acknowledge the **foundational importance of frameworks** that ensure **ethical and responsible use of personal data**, including those **enabling privacy and ensuring personal data protection**, **digital security**, and **promoting the interoperability** and **governance of health data")** (G20, 2020[24]).
- the Global Digital Health Partnership is developing a Model Security Notice in 2023 to harmonise digital security requirements for technology developers, lower cost, and risk for governments, and to clearly convey information to patients and users about digital security controls (Gobal Digital Health Partnership, 2023[25]).
- the World Health Organisations' (World Health Organisation, 2021[26]) includes cooperation and collective action better use digital tools and technologies, including artificial intelligence, while ensuring appropriate security and privacy protections are in place.

125. Digital security is increasing in its importance in health to match the growth of digitalisation. As seen above, most OECD countries are taking action to strengthen their approach to digital security and there is opportunity for greater collaboration which will help efforts within and across countries.

126. Furthermore, the approach to digital security is not unique to health. Collaboration with other industries to share insights in the public interest, such as enhancing digital literacy among the public and adopting emerging strategies to mitigate digital security risks, presents an opportunity. The healthcare sector generally has a lower level of maturity in the field of cybersecurity and higher budgetary constraints than other industries (such as finance). Achieving a mutually beneficial arrangement across sectors may not be straightforward; however, there are three key priority areas for collective efforts across sectors that fortify the digital security foundation.

127. **Priority 1: Strengthen alignment between digital security approaches in health with overall digital security strategies.** Countries should continue to build on the OECD digital security risk management framework (aligned with the OECD Recommendation on Health Data Governance) to strengthen their approach to digital security in health toward leading practices as identified in Table 3.12. Countries should take more pro-active steps in improving digital security culture (engaging in training and simulating phishing and cyberattacks to test response effectiveness), strategy and governance (aligning overall risk management programs, allocating 10% of IT budgets to security), and risk management (monitoring and reporting digital security risks more frequently).

128. **Priority 2: Enhance co-operation in areas of mutual benefit, such as enabling a digital security culture, strengthening strategy and governance, and embedding risk assessment and treatment in regular reporting:** Countries should cooperate in knowledge sharing and co-development of leading practices within and across borders and with other industries. Further, countries should share intelligence and information sharing about cyberthreats and cyberattacks to help each other prepare, detect, and act.

129. **Priority 3: Collaborate on innovative and emerging tools:** Countries could collaborate on innovation and emerging tools in threat detection and security management to determine their efficacy and methods for implementation. Common innovations being implemented are identity management, multi-factor authentication, role-based access, and applying encryption for data at rest and in motion. Emerging tools include zero-trust approaches, synthetic data, and applying Block Chain.

Annex A. Tables of country responses of the questionnaire

130. The tables below contain country specific responses to the questions in the OECD digital health security questionnaire. These tables were created after the original questionnaire to summarise their responses and to better align with the summary presented in Table 3.12

131. Note that as part of the questionnaire, respondents were asked to consider three use cases when answering the questionnaire. The first use case was about digital security in the communication and use of data about individuals in testing, contact tracing, or vaccination status. Second was about digital security in the use of aggregate data for reporting on COVID-19 case counts or rates of vaccination that may have been disaggregated by socio-demographic factors. Third was in digital security for the storage, display, and sharing of vaccine certificates. In most responses, there was no difference across use cases. These responses have been included below.

Table 0.1. Australia answers to digital health security questionnaire

132. **Australia's** response was co-authored by the Australian Digital Health Agency and the Australian Department of Health and Aged Care.

- The **Australian Digital Health Agency** focuses exclusively on digital health and manages the "*My Health Record* system" (a national electronic health record) and oversees the implementation of the national Digital Health Cyber Security Strategy, which encompasses both Federal and State/Territory entities as well as public and private healthcare providers.
- The **Department of Health and Aged Care** has broad responsibility for the governance and coordination of Australia's healthcare system, and manages the "*Electronic-Prescription System*", which was implemented as a part of the nation's COVID-19 response.

133. The Australian Digital Health Agency has a cybersecurity strategy that covers government and non-government owned health infrastructure. A notable aspect of the Australian system is that part of their health system is funded and managed by and within territories and delivered by thousands of private sector health organisations. The Australian Digital Health Agency provides information and guidance to consumers and the healthcare sector to help keep information secure (https://www.digitalhealth.gov.au/initiatives-and-programs/cyber-security). Australia has also collaborated with other countries on digital security, for example by participating in the Global Digital Health Partnership (GDHP) and Health Information Sharing and Analysis Center (H-ISAC).

134. For regulated digital health solutions, such as the Electronic Prescribing System, there are specific 'conformance schemes' that allows conformant products (in public and private sectors) to participate in the digital health ecosystem. The COVID pandemic did not fundamentally change Australia's security requirements, although it did increase the health sectors reliance on digital health technologies.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes**
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Phishing simulations, refresh training, awareness, and other engagements
Are there defined key roles and responsibilities within organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Federal Government and Cyber Security Centre
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs regarding digital security protection for the public?	Yes
Who is in charge of the digital literacy programs?	The Australian Digital Health Agency have training modules and information
Are there standard communication plans for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Does the security program include communications across organisations?	Yes
Is managing digital security risk is part of an overall approach to risk management?	Yes
Is risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	Yes

Amount	Distinct and prominent part of the ADHA budget
The organisation is accountable for the system and is monitoring the security	Yes
Frequency	Continuously monitoring**
There is a pro-active program for security measures	Yes
Pro-active measures	Patching, multi-factor authentication, audit logs, firewalls, regular anti-virus scanning, system monitoring
There is regular reporting of the performance of the digital security program	Yes
Frequency	Confidential
Method	Confidential
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Identity management, multifactor authentication, data encryption
There are clear accountabilities and escalations plans in place in case of a cyberattack or intrusion	Yes
What types of plans are in place?	Business continuity and disaster recovery plans. No paper-based plans, individual clinics may access relevant data though local systems
There are periodic security intrusion and response tests to test effectiveness of security	Yes
What methods are used	Confidential

Note: **there might be variation between state and private health organisations

Table 0.2. Belgium answers to digital health security questionnaire

135. **Belgium** collected data in a centralized national database used for policy-supporting research/statistics named '*Coronalert.'* This dataset contained pseudonymized data on COVID-19 rates, vaccinations and demographic information on geography, gender, age, and other factors.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Partly
Is there a common curriculum?	No
Are there pro-active measures?	Yes
What are types of pro-active measures?	Regular topic in monthly meeting
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Partly
Who is the coordinator?	n.r.
Is there a public participation approach in understanding public requirements for digital security?	n.r.
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	n.r.
Are there a standard communication plan for impacted parties in the case of a security breach?	No
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	No
Is managing digital security risk a part of an overall approach to risk management?	Partly
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	Partly
Amount	
Is the organisation accountable for the system and is monitoring the security	Yes
Frequency	Monthly
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching
There is regular reporting of the performance of the digital security program?	No
Frequency	N.r.
Method	n.r.
Innovations	Encryption data in motion and rest, role base access, and plan for cloud-based integration
Are there clear accountabilities and escalations plans?	Yes
What types of plans are in place?	Continuity plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Non-periodic

Table 0.3. Canada response to digital security in health questionnaire

136. **Canada** have responded based on their general approach to digital security for national public health. Canada has local jurisdictions for digital health information where the provinces and territories manage digital security within their respective remits. On the national level, Canada has a national digital security in health program derived from a Government of Canada policy, which aligns its activities to meet their National Cyber Security Strategy. Oversight of digital health is primarily led within each province and territory. Canada is exploring a federated health data management approach.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Partly
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Phishing stimulations, security awareness and guidance
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Government of Canada Policy
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	Canadas Centre for Cyber Security
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	Yes
Amount	n.r.
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuously monitoring
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching, vulnerability management, continuous security verification activities.
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Annual
Method	Wide cybersecurity assessment reporting (w/other agencies)
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Investment in new and emerging security technologies
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	IT continuity plans, business recovery and disaster recovery
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Periodic reviews

Table 0.4. Costa Rica response to digital security in health questionnaire

137. **Costa Rica** has responded on their overall approach to digital security in health, as has been established following their response to the 2022 cybersecurity incident.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Partly
Is there a common curriculum?	No
Are there pro-active measures?	Yes
What are types of pro-active measures?	Awareness
Are there defined key roles and responsibilities within the organisations?	Partly
Is there a national digital security in health program that aligns peer organisations?	No
Is there a coordination actor or institution?	Partly
Who is the coordinator?	Ministry of Science and Technology
Is there a public participation approach in understanding public requirements for digital security?	n.a.
Is there a digital literacy- programs for digital security directed at the public?	no
Who is in charge of the digital literacy programs?	
Are there a standard communication plan for impacted parties in the case of a security breach?	no
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	No
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	No
Amount	n.a.
Is the organisation accountable for the system and is it monitoring the security?	No
Frequency	Applied against demand
Are there a pro-active program for security measures?	Yes
Pro-active measures	
Is there regular reporting of the performance of the digital security program?	No
Frequency	n.a.
Method	n.a.
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Paper based
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Not periodic

Table 0.5. Croatia response to digital security in health questionnaire

138. **Croatia** reported based on its "*Central Platform for Registration of COVID-19 Testing*", a centralised national information system. This platform monitors and reports data on infectious disease. In Croatia, there is no national program for digital security in health, but there are strategic documents for cybersecurity and the Ministry of Health which oversees the implementation of security measures in the digital health sphere. As there is a general digital security strategy where the National Security Council serves as a single point of contact for digital security. Croatia cooperates with other European countries on cybersecurity in health and data exchange projects. In response to the COVID-19 pandemic, Croatia has implemented a rapid information exchange channel and an additional initiative to protect hospitals.

Question	Answer
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	No
Is there a common curriculum?	No
Are there pro-active measures?	Yes
What are types of pro-active measures?	Awareness
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	National Security Council framework
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes, but not by health services
Who is in charge of the digital literacy programs?	National Security Council have education programs and workshops for public sector officials
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	No
Amount	Funding is given to specific projects (procurement of specific requirements, such as firewalls antivirus solution etc. Otherwise, funding is based on EU
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Periodic (usually annual) vulnerability scanning, from 2020 there were additional protection through a monitoring program.
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching, antivirus and anti-spam software, IT equipment's updates
Is there regular reporting of the performance of the digital security program?	No
Frequency	Ad-hoc

Method	Reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Mandatory VPN, smart cards for health professionals, state-owned PKI infrastructure, authentication, authorization, role-based access, audit logging, non-repudiation digital signaling, enforced encryption.
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Paper based
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Ahead of platform launching

Table 0.6. Czech Republic response to digital security in health questionnaire

139. **Czechia** reported on its "*National Register of International Securities Identifying Numbers* (ISIN)". This is a centralised national system composed of different elements of healthcare, such as making appointments and other mobile applications for citizens. Czechia's National Digital Security Strategy for health and the National Cyber and Information Security Agency provide guidance and oversight in digital security in health for over 70% of health providers. Digitalisation projects have been delayed as a result of the COVID-19 pandemic.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	No
What are types of pro-active measures?	
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	National Cyber and Information Security Agency
Is there a public participation approach in understanding public requirements for digital security?	No
Is there a digital literacy- programs for digital security directed at the public?	No
Who is in charge of the digital literacy programs?	
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	No
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	No
Amount	Funding is provided for specific projects and through EU funding
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuous monitoring
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Annually

Method	Reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Identity management, multifactor identification, encryption for data in rest and motion, synthetic data, role-based access, managed network, monitoring, security log correlation, geographical redundance
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business Impact Assessment and Business Continuity Management Plans, theoretical paper based
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Test major changes

Table 0.7. Greece response to digital security in health questionnaire

140. **In Greece** it is the Ministry of Health and Ministry of Digital Governance who are the authorities for digital security in health**;** however, there are currently not specific program for digital security in health. Still, their digital transformation of health program includes subprojects for digital security in health. The Covid-19 pandemic has demonstrated the need of systematic digital security measures and legal framework for Greece, which they – In cooperation with other EU members – are developing. They will be responding to the questioner with their National COVID-19 registry – a registry that includes test results, vaccinations status and hospitalisation data.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	No
What are types of pro-active measures?	
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	National Cyber and Information Security Agency
Is there a public participation approach in understanding public requirements for digital security?	No
Is there a digital literacy- programs for digital security directed at the public?	No
Who is in charge of the digital literacy programs?	
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	No
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	No
Amount	Funding is provided for specific projects and through EU funding
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuous monitoring
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Annually
Method	Reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Identity management, multifactor identification, encryption for data in rest

	and motion, synthetic data, role-based access, managed network, monitoring, security log correlation, geographical redundance
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business Impact Assessment and Business Continuity Management Plans, theoretical paper based
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Test major changes

Table 0.8. Ireland response to digital security in health questionnaire

Questions	**Answers**
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	There is Cyber Security Awareness training that covers key items related to security and cyber
Are there pro-active measures?	Yes.
What are types of pro-active measures?	Proactively we conduct phishing simulations every two months across the entire organisation. We track the results and use this to inform our awareness and training plan. In addition, we have 24x7 security operations in place which proactively monitor and detect any suspicious activity on our network, servers, and end points.
Are there defined key roles and responsibilities within organisations?	We have a CISO organisation that is responsible for Digital Security. This CISO organisation has defined key roles and responsibilities aligned with industry best practice.
Is there a national digital security in health program that aligns peer organisations?	We have established a national programme for ICT & Cyber programme which is run by the HSE that is responsible for improving our Cyber and Security posture.
Is there a coordination actor or institution?	The ICT & Cyber programme is under the remit of the Chief Technology and Transformation Officer of the HSE.
Who is the coordinator?	The HSE is the coordinator of the programme
Is there a public participation approach in understanding public requirements for digital security?	The basis of the ICT & Cyber programme is derived from the HSE's Post Incident Review that was made public in December 2021. We have a number of patient body engagement forums for which Digital security may be covered but it is not the prime focus of the engagement.
Is there a digital literacy- programs regarding digital security protection for the public?	The HSE does not run a digital security program for the public. This would fail under the remit of our National Cyber Security Centre which is under the Department of Environment, Climate and Communications.
Who is in charge of the digital literacy programs?	The Department of Environment, Climate and Communications
Is there a standard communication plan for impacted parties in the case of a security breach?	Yes – we have a Cyber Incident Playbook
Is there a program in place to communicate potential threats internally?	Yes – we we have a Cyber Threat

	Dashboard under the management of the CISO organisation which is used communicate Cyber threats internally
The security program includes communications across organisations?	Yes
Is managing digital security risk is part of an overall approach to risk management?	Yes – Digital Security is on our corporate risk register
Is risk management approach is aligned across organisations?	The HSE has a defined approach to Enterprise Risk Management
Is there a distinct budget for digital security?	Yes
Amount	Undisclosed.
The organisation accountable for the system is monitoring the security	The CISO organisation within the HSE is monitoring the security. We have also completed an independent reassessment of Cyber Maturity by a third party.
Frequency	Our independent reassessment is yearly
There is a pro-active program for security measures	The Cyber program is aligned to NIST CSF, in addition to improving Cyber defenses we are also focused on legacy renewal to reduce the potential attack surface for cyber threats.
Pro-active measures	Legacy renewal, migration to cloud and an active threat and vulnerability management programme are 3 core tenants of our pro-active measures
There is regular reporting of the performance of the digital security program	Yes – there is significant governance in place
Frequency	We have steering monthly, we also report progress to a subcommittee of the board of the HSE, and also report progress to the NCSC on a number of relevant matters under the NIS Directive.
Method	Program progress reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Our overall programme is designed around key six areas: ICT & Cyber governance Compliance Security Operations Foundational Technology Threat and Vulnerability Management IT Service and Asset management In addition, for each initiative under these 6 areas we have aligned our workplans to the NIST Cyber Security fiver domains: identify, protect, detect, respond, and recover.
There are clear accountabilities and escalations plans in place in case of a cyberattack or intrusion	Yes
What types of plans are in place?	We have a Cyber Incident Response playbook
There are periodic security intrusion and response tests to test effectiveness of security	We conduct penetration tests on new software releases, in addition our threat and vulnerability management approach will introduce proactive and ongoing assessments of vulnerabilities in our environment on an ongoing and continuous basis.
What methods are used	Penetration Tests

Table 0.9. Israel response to digital security in health questionnaire

141. **Israel** described their "*Centralised National System for Aggregated Data on the Pandemic*". This platform stores data for epidemiological research, transferring data between agencies. The platform is also used for evidence-based decision making. Overall, it is the Ministry of Health's Cybersecurity Program which oversees digital security in health. The programme is based on the framework established by the Israel National Cyber Directorate. As part of the plan, all organisations are required to commit to and support the cybersecurity initiative and are regularly supported (free of charge) from the Ministry of Health. In addition, during COVID-19, they increased their supply chain control, home care, and cloud-based services.

Questions	Answer
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Phishing simulations, reporting and awareness
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Ministry of Health and National Cyber Directorate
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	Survey digital literacy as a part of the project for digital literacy
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	Yes
Amount	8% of the IT budget
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuously
Are there a pro-active program for security measures?	Yes
Pro-active measures	Risk assessment evaluation
Is there regular reporting of the performance of the digital security program?	n.r.
Frequency	n.a.
Method	n.a.
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Multi-factor identification, encryption for data in rest and motion, synthetic data, role-based access, cloud technology
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Disaster Recovery Plans and Business continuity plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used?	Annually

Table 0.10. Italy response to digital security in health questionnaire

142. **Italy** presented their "*Electronic Health System*" (FSE). In Italy, each region collects health data and reports regularly to the Health Ministry. The national cybersecurity strategy provides the framework for digital security in health, including the legal framework for data privacy and security. Furthermore, the National Point of Contact is responsible for coordinating security measures and is the main contact to the European Commission. Italy is in the process of introducing health innovations into its health system, including digital platforms for collecting, sharing, and analysing data. The digitalisation of health increased during the COVID pandemic – and Italy is working to ensure the security of these platforms.

Questions	Answers
Is there a program for security training within the organisation?	No**
Is the training is periodically refreshed?	n.a.
Is there a common curriculum?	No**
Are there pro-active measures?	Yes
What are types of pro-active measures?	Refresh training, cyber pills, and awareness
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	
Is there a public participation approach in understanding public requirements for digital security?	Yes**
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	Plan for increased digital literacy among students and teachers, online learning modules, non-profit organisations working on digital literacy, promoting digital culture thought awareness of cyber risk.
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	n.r.
Amount	
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Periodically dependent of type of threat, level of risk and sensitivity of the data.
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching, updates, reviews
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Continuously
Method	
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Multi-factor authentication, Encryption, backup and disaster recovery, Firewalls, Intrusion Detection, Preventive systems, regular security audits
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Disaster Recovery Plans and Business Continuity Plan
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Quarterly or semi annual

Note: **note of that there is no current program, but it is being implemented, **public requirement through laws and regulations

Table 0.11. Japan response to digital security in health questionnaire

143. In **Japan,** the Digital Agency and the Ministry of Health, Labour and Welfare are responsible for the digital security in health. They are establishing common standards for cybersecurity across government agencies and peer-organisations. During the COVID pandemic they developed and implemented a vaccination app and a system for vaccination records. In addition, the pandemic also influenced their adoption of a zero trust[3] approach to policy.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes, annually
Is there a common curriculum?	N.r.
Are there pro-active measures?	
What are types of pro-active measures?	
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	N.r.
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	N.r.
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	N.r.
Do the risk management approach is aligned across organisations?	N.r.
Is there a distinct budget for digital security?	N.r.
Amount	N.r.
Is the organisation accountable for the system and is monitoring the security	Yes
Frequency	Continuously
Are there a pro-active program for security measures?	N.r.
Pro-active measures	N.r.
There is regular reporting of the performance of the digital security program?	Yes
Frequency	Continuously
Method	
Innovations	
Are there clear accountabilities and escalations plans?	Yes
What types of plans are in place?	N.r.
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Ad-hoc

[3] **Zero Trust** assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. <REF Zero Trust Architecture | NIST>

Table 0.12. Korea response to digital security in health questionnaire

144. **Korea** provided information about "*The COVID-19 Information Management System*", which is a system for tracking vaccinations. Overall, there is no programme for digital security in health; however, the Ministry of Health follow the National Information Security Guidelines. This includes training of staff in cybersecurity. The COVID pandemic mainly affected private medical institutions, with the Ministry of Health supporting installations of anti-ransomware for vaccine providers.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Education, training, vulnerability checks, simulation exercise
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Internal - department of information security
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	Training and manuals
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	Yes
Amount	10% of digitalisation budget
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuously monitoring and audits once a year
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching and monthly checking of computers
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Monthly
Method	Reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Public authentication, simple authentication, OTP, apply blockchain encryption (COOV system) and cloud-based technology
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Disaster recovery Plan, backup and dissipate data
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Annually

Table 0.13. Lithuania response to digital security in health questionnaire

145. **Lithuania** gave examples from "*The Centralised National e-Health Systems*". In these registers, processors can connect to patient registers and patients can connect to their health registers (prescriptions, dispensations, laboratory results, medical images, hospital discharges, COVID-19 certificates and more). There is no health specific digital security programme, so the health sector follows the national law on cybersecurity which is based on European Union directives.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	No
Are there pro-active measures?	Yes
What are types of pro-active measures?	Training
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	National Cyber Security Center
Is there a public participation approach in understanding public requirements for digital security?	No
Is there a digital literacy- programs for digital security directed at the public?	No
Who is in charge of the digital literacy programs?	n.a.
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Partly
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	Yes
Amount	12.3% of IT budget (1.2 million)
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Report once a month and scan systems every other day
Are there a pro-active program for security measures?	Yes
Pro-active measures	Recommended updates once a week
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Annually
Method	Reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Multi Factor authentication, Role based access
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Digital format transferred with delay (worst case scenario)
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Annually

Table 0.14. Luxembourg response to digital security in health questionnaire

146. **Luxembourg** replied that their `snapshot` covered multiple systems owned by multiple organisations (hospitals, the national digital health agency and a BI system operated by the ministry of Health); and as such they are not managed by a single entity or a single "rulebook". Luxembourg does not yet have a national digital security in health program, but regularly monitor digital security in health. In response to the pandemic, Luxembourg is in the process of implementing a central governance of digital security in health, which covers initially the hospital sector through the set-up of a SOC for the health sector.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Partly
Are there pro-active measures?	Yes
What are types of pro-active measures?	Staff meeting (monthly), awareness
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Organ for secure information
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Not by health services
Who is in charge of the digital literacy programs?	Programs run by non-health organisations
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	Yes
Amount	n.r.
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Once a year and real-time monitoring
Are there a pro-active program for security measures?	Yes
Pro-active measures	n.r.
Is there regular reporting of the performance of the digital security program?	Partly
Frequency	Varies
Method	
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Identity management, multi-factor authentication, Encryption for data at rest and in motion, synthetic data, role-based access, cloud technologies
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes*
What types of plans are in place?	Each hospital has their own plans, for Covid system there is a pandemic continuity plan, DRP plans and on call service.
There are periodic security intrusion and response tests to test effectiveness of security?	Varies
What methods are used	Annually (eSante)

Table 0.15. Netherlands response to digital security in health questionnaire

147. **Netherlands** replied based on their 'CoronaCheck' digital platform that is based on a decentralized data-infrastructure where important stakeholders including commercial, healthcare providers, and government bodies can process decentralized COVID 19-related health data, including test results, vaccination results, and exemptions. For more efficient data-processing, there are centralized systems in place to perform other key functions, such as generating digital certificates, all while providing strong security and privacy. More recently, a Contract Tracing digital application has been implemented in Netherlands which is managed via a centralized municipality.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	No
Are there pro-acitve measures?	Yes
What are types of pro-active measures?	Open communication and regular monitoring
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Partly
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Ministry of Health, Welfare, and Sports
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	No
Who is in charge of the digital literacy programs?	-
Are there a standard communication plan for impacted parties in the case of a security breach?	No
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	Yes
Amount	15% of all IT costs
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuous monitoring
Are there a pro-active program for security measures?	Yes
Pro-active measures	Penetration tests and patches
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Monthly
Method	Failure Mode Effect Analysis (FMEA)
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Multiple methods
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business continuity plans and third-party storage of logs and backup data for recovery
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	In the event of changes to infrastructure and ad-hoc

Table 0.16. Norway response to digital security in health questionnaire

148. **Norway** responded with "Monitoring and Reporting Data Security" in mind. Norway has a national cross-sectoral strategy for digital security. The present strategy is Norway's fourth cyber security strategy and is intended to address the challenges that will inevitably arise in conjunction with the rapid and far-reaching digitalisation of the Norwegian society. In health there is a Code of conduct for information security and data protection, which consists of a set of requirements that apply to the entire health sector and major institutions, which is continuously updated. Each organisation is responsible for its own digital security. This is illustrated by the fact that both the Norwegian Board of Health and the National Security Authorities have oversight of digital security in Norway, and within the health sector. During the pandemic Norway introduced several digital services and applications, such as a COVID certificate app and a notification app for COVID.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Regular e-learning, awareness
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	The Norwegian Digitalisation Agency and Directorate of e-Health
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Not by health services
Who is in charge of the digital literacy programs?	The Norwegian Center for Information Security provides information and support
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Partly
Is there a distinct budget for digital security?	Partly
Amount	Digital security is included in the IT budget, but there are distinct budgets for initiatives (e.g., Security awareness training)
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Vulnerability assessment weekly basis, central system reports every six months
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching
Is there regular reporting of the performance of the digital security program?	Partly**
Frequency	
Method	
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Multi-factor authentication, zero-trust, micro-segmentation, endpoint security monitoring, encryption.
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	

There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Non-regular

Note: ** the main data processor, NHN, provide monthly reports on security related issues.

Table 0.17. Portugal response to digital security in health questionnaire

149. **Portugal** provided responses based on their digital platform called *"TraceCOVID"*, where healthcare professionals can register to share COVID-19 results in a secure and reliable way. There were several systems monitoring and reporting COVID-19 related data; however, only one of them has COVID-19 related data and demographic data. In Portugal, there are several laws and regulations on cybersecurity, albeit nonspecific to health.

Question	Answer
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	No
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Documents
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Coordinator Council of Information Security in Health
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	Portuguese Safe Internet Centre promote safe and responsible internet and technology use
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	Yes
Amount	Specific budget, that also include IT and HR
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Frequency dependent on organisation and level of risk
Are there a pro-active program for security measures?	Yes
Pro-active measures	Proactive vulnerability scanning
Is there regular reporting of the performance of the digital security program?	n.r.
Frequency	
Method	
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	no
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business Continuity and disaster recovery plan, some cases there are paper-based plan
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	non-regular

Table 0.18. Slovak Republic response to digital security in health questionnaire

150. **The Slovak Republic** based their answers on two systems: '*The National eHealth System'* and '*Public Health Authority Information System'*. They apply data security assessments on their core Health systems, but report neither having a digital security program nor oversight programme. They are improving their security of public health in response to the recent COVID pandemic.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	No
Are there pro-active measures?	Yes
What are types of pro-active measures?	Monitoring, official periodic audit
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	No
Is there a coordination actor or institution?	No
Who is the coordinator?	-
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	National Cybersecurity Center raise awareness
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	no
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	Yes
Amount	EU fund specific for security projects
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	SIEM
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching and vulnerability scanning
Is there regular reporting of the performance of the digital security program?	No
Frequency	n.r.
Method	Reports
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	no
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business Continuity and Disaster Recovery Plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	n.r.

Table 0.19. Slovenia response to digital security in health questionnaire

151. **Slovenia** focussed on its '*Centralised Health Information System – eHealth*'. This system connects local information systems of healthcare service providers to centralised information solutions and databases. Digital security is part of organisational strategy and requirements of specific national laws. The Government Information Security Office oversees compliance with legal requirement regarding information security.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	No
Are there pro-active measures?	Yes
What are types of pro-active measures?	Training and awareness
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Partly
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Government Information Security Office, Ministry of Health, and National Institute of Public Health
Is there a public participation approach in understanding public requirements for digital security?	Partly
Is there a digital literacy- programs for digital security directed at the public?	Not by health services
Who is in charge of the digital literacy programs?	n.r.
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	No
Amount	
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Continuously monitoring.
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Daily
Method	Reporting
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Identity management, multi factor authentication, encryption for data in motion
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business Continuity and Disaster Recovery Plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Annually

Table 0.20. Spain response to digital security in health questionnaire

152. **Spain** replied based on their central system and registry for COVID vaccination certificates. In general, they have the National Security Scheme (ENS) which is compulsory for all public administration organisation regardless of level (National, Regional, or Local). However, Spain also adheres to the General Data Protection Regulation (GDPR) from the EU. In regard to their vaccine certificates are Spain using a public key cryptology scheme to protect the health information, as required by GDPR. In response to the pandemic, Spain have increased focus on digital security in health.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Security pills
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	National Cryptology Centre
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Not by Health services
Who is in charge of the digital literacy programs?	Spanish National Cybersecurity Institute (INCIBE) and CCN-CERT
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Yes
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	No
Amount	
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Annual audits
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patches, audits
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	Annual
Method	Report
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	Multiple methods
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	ITC continuity and Disaster Recovery Plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	n.r.

Table 0.21. Switzerland response to digital security in health questionnaire

153. **Switzerland** has the '*National Electronic Patient Record*' and the system for vaccination and contract tracing system during COVID-19. Their general cyber security is managed by the National Cyber Security Centre and all government projects are subject to the same security requirements. Security is monitored according to the level of security needed. For health projects, it is the Federal Office of Public Health that oversee digital security. In retrospect, Switzerland has learned from the COVID pandemic the importance of personal data protection, cross-border cooperation in health security, and sub-national cooperation.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	No
Is there a common curriculum?	No
Are there pro-active measures?	No
What are types of pro-active measures?	
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	National Cyber Security Center
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy program in digital security directed at the public?	Yes
Who oversees the digital literacy programs?	National Cyber Security Centre
Are there a standard communication plan for impacted parties in the case of a security breach?	No
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	Partly**
Do the risk management approach is aligned across organisations?	Yes
Is there a distinct budget for digital security?	No
Amount	
Is the organisation accountable for the system monitoring the security?	Yes
Frequency	Required before major changes
Are there a pro-active program for security measures?	Yes
Pro-active measures	n.r.
Is there regular reporting of the performance of the digital security program?	Yes
Frequency	n.r.
Method	n.r.
In the organisation accountable for the system, what are leading and emerging methods that are being applied to improve digital security?	
Are there clear accountabilities and escalations plans in place in case of a cyberattack or intrusion?	Yes
What types of plans are in place?	Business Continuity Plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	non-regular

Table 0.22. The United Kingdom response to digital security in health questionnaire

154. The **United Kingdom** have recently launched a national digital security in health programme. In addition, the *Security of Network and Information Regulations* stipulate that organisations must assess their systems annually. During the pandemic the UK government issued an inquiry on the delivery of health. In the aftermath of the pandemic, it has directed health towards technical innovation, such as normalising video calls with health providers. The UK prioritises key organisations having adequate digital security as well as alignment across organisations. In the response to the current questionnaire, the United Kingdoms approached each country within the UK for comments to reflect their approach to cyber security is reflected. Overall, Scotland have noted some differences from Northern Ireland, England, and Wales.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Yes
Is there a common curriculum?	Yes
Are there pro-active measures?	Yes
What are types of pro-active measures?	Training, campaigns, and phishing
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Security of Network and Information System Regulations and Government Health and Social Care Directorates
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	n.r.
Who is in charge of the digital literacy programs?	n.r.
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	No
Do the risk management approach is aligned across organisations?	No
Is there a distinct budget for digital security?	Yes
Amount	n.r.
Is the organisation accountable for the system and is monitoring the security	Yes
Frequency	Annually
Are there a pro-active program for security measures?	Yes
Pro-active measures	Continuous monitoring
There is regular reporting of the performance of the digital security program?	N.r.
Frequency	N.r.
Method	N.r.
Innovations	Secure backup data
Are there clear accountabilities and escalations plans?	Yes
What types of plans are in place?	Continuity and disaster recovery plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	Non-regular

n.b. these countries are pending their questionnaire responses due to complexity and confidentiality. In table3.1, their responses have been tagged as "I".

Table 0.23. The United States response to digital security in health questionnaire

155. In **the United States** the Department of Health and Human Services Office of Civil Rights provide guidance and resources for digital security in health and implementation is decentralized and local. Meanwhile, it is the Department of Commerce, National Institute of Standards and Technology who outline the framework on cybersecurity.

Questions	Answers
Is there a program for security training within the organisation?	Yes
Is the training is periodically refreshed?	Partly. Security training is periodically reviewed and updated as required
Is there a common curriculum?	n.a.
Are there pro-active measures?	Yes
What are types of pro-active measures?	Awareness, training programs, safeguarding passwords
Are there defined key roles and responsibilities within the organisations?	Yes
Is there a national digital security in health program that aligns peer organisations?	Yes
Is there a coordination actor or institution?	Yes
Who is the coordinator?	Health Insurance Portability and Accountability ACT (HIPAA) Security Rule
Is there a public participation approach in understanding public requirements for digital security?	Yes
Is there a digital literacy- programs for digital security directed at the public?	Yes
Who is in charge of the digital literacy programs?	n.r.
Are there a standard communication plan for impacted parties in the case of a security breach?	Yes
Is there a program in place to communicate potential threats internally?	Yes
Is there a security program that includes communications across organisations?	Yes
Is managing digital security risk a part of an overall approach to risk management?	
Do the risk management approach is aligned across organisations?	
Is there a distinct budget for digital security?	n.a.
Amount	
Is the organisation accountable for the system and is monitoring the security	Yes
Frequency	No prescribed frequency, but HIPAA requires that processes are implemented to prevent, detect, contain, and correct security violations
Are there a pro-active program for security measures?	Yes
Pro-active measures	Patching
There is regular reporting of the performance of the digital security program?	Yes
Frequency	Continuously
Method	Multiple agencies communicate security threats
Innovations	n.r.
Are there clear accountabilities and escalations plans?	n.a.
What types of plans are in place?	Contingency and disaster recovery plans
There are periodic security intrusion and response tests to test effectiveness of security?	Yes
What methods are used	No prescribed frequency

References

Anderson, J. (2023), *Global cyberattacks increased 38% in 2022*, https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022. [12]

Deloitte (2023), *2023 Global Future of Cyber Survey*, https://www.deloitte.com/content/dam/assets-shared/legacy/docs/gx-deloitte_future_of_cyber_2023.pdf>. [18]

Deloitte (2020), *91% of all cyber attacks begin with a phishing email to an unexpected victim*, https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html. [5]

Department of Health and Social Care (2018), "Lessons learned review of the WannaCry Ransomware Cyber Attack", *Department of Health & Social Care* February. [27]

G20 (2020), *G20 Health Ministers' Declaration*, https://ezcollab.who.int/file2.axd/7wbpfqm6.kg7pslj3/G20%20Health%20Ministers%20Declaration_EN_%2020>. [24]

Garrity, M. (2019), *5% of IT budgets go to cybersecurity despite 82 of hospitals reporting breaches*, https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html. [20]

Gobal Digital Health Partnership (2023), *A Global Commitment to Digital Health*, https://gdhp.health/. [25]

Hughes, O. (2018), *Norway healthcare cyber-attack 'could be biggest of its kind'*, https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/. [7]

kaspersky (n.d.), *What is WannaCry ransomware?*, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. [16]

Mckinsey and Company (2023), *What is cybersecurity?*, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity. [2]

OECD (2022), *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity | READ online*, https://read.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en#page1 (accessed on 26 January 2023). [6]

OECD (2022), *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en. [3]

OECD (2022), *Recommendation of the Council on Digital Security Risk Management, OECD/LEGAL/0479*. [14]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463*. [23]

OECD (2021), "Smart policies for smart products: A policy maker's guide to enhancing the digital security of products", Directorate for Science, Technology and Innovation Policy Note, OECD, Paris,", http://www.oecd.org/digital/smart-policies-for-smart-products.pdf. [1]

OECD (2017), *Recommendation of the Council on Health Data Governance, OECD/LEGAL/0433*. [4]

OECD (1997), *Recommendation of the Council concerning Guidelines for Cryptography Policy, OECD/LEGAL/0289*. [22]

Samtani, S. (2022), *How AI is shaping the cybersecurity arms race*, https://theconversation.com/how-ai-is-shaping-the-cybersecurity-arms-race-167017>. [21]

SenseOn (2022), *How Much Should a Business Spend on Cybersecurity?*, https://www.senseon.io/resource/how-much-should-a-business-spend-on-cybersecurity/. [19]

Smart, W. (2018), *Lessons learned review of the WannaCry Ransomware Cyber Attack*. [15]

Sobers, R. (2022), *166 Cybersecurity Statistics and Trends [updated 2022]*, https://www.varonis.com/blog/cybersecurity-statistics. [13]

Solomon, H. (2023), *Management, lack of money blamed for poor cybersecurity at Canadian hospitals*, https://www.itworldcanada.com/article/management-lack-of-money-blamed-for-poor-cybersecurity-at-canadian-hospitals/527412. [8]

Stephends, J. (2020), *Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak*, https://brnodaily.com/2020/03/13/news/serious-cyber-attack-targets-brno-university-hospital/. [9]

The Lancet Digital Health (2021), "Digital technologies: a new determinant of health", *The Lancet Digital Health*, Vol. 3/11, p. e684, https://doi.org/10.1016/s2589-7500(21)00238-7. [17]

Tidy, J. (2021), *Irish cyber-attack: Hackers bail out Irish health service for free*, https://www.bbc.com/news/world-europe-57197688. [10]

Witts, J. (2023), *Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know*, https://expertinsights.com/insights/healthcare-cyber-attack-statistics/. [11]

World Health Organisation (2021), *Global strategy on digital health 2020-2025*, https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf. [26]

OECD Health Working Papers

A full list of the papers in this series can be found on the OECD website:

https://www.oecd.org/health/health-working-papers.htm

No. 163 - EXAMINING RECENT MORTALITY TRENDS – THE IMPACT OF DEMOGRAPHIC CHANGE (November 2023) David Morgan, Paul Lukong, Philip Haywood and Gabriel Di Paolantonio

No. 162 - UNDERSTANDING INTERNATIONAL MEASURES OF HEALTH SPENDING: AGE-ADJUSTING EXPENDITURE ON HEALTH (October 2023) David Morgan and Michael Mueller

No. 161- ASSESSING THE FUTURE FISCAL SUSTAINABILITY OF HEALTH SPENDING IN IRELAND (September 2023) Luca Lorenzoni, Pietrangelo de Biase, Sean Dougherty and Tiago McCarthy

No. 160- ELECTRONIC HEALTH RECORD SYSTEM DEVELOPMENT, DATA USE AND GOVERNANCE: SURVEY RESULTS (September 2023) Luke Slawomirski, Luca Lindner, Katherine De Bienassis, Philip Haywood, Tiago Cravo Oliveira Hashiguchi, Melanie Steentjes and Jillian Oderkirk

No. 159 - PATIENT ENGAGEMENT FOR PATIENT SAFETY (September 2023)
Candan Kendir, Rie Fujisawa, Óscar Brito Fernandes, Katherine de Bienassis and Niek Klazinga

No. 158 - VALUE-BASED PAYMENT MODELS IN PRIMARY CARE: AN ASSESSMENT OF THE MENZIS SHARED SAVINGS PROGRAMME IN THE NETHERLANDS (June 2023) Luca Lindner and Arthur Hayen

No. 157 - DEVELOPING A SET OF INDICATORS TO MONITOR THE PERFORMANCE OF THE PHARMACEUTICAL INDUSTRY (August 2023) Rishub Keelara, Martin Wenzl, Lisbeth Waagstein, Marjolijn Moens and Ruth Lopert

No. 156 - ENHANCING COMPETITION IN ON-PATENT MARKETS (June 2023) Eliana Barrenho, Marjolijn Moens, Lisbeth Waagstein and Ruth Lopert

No. 155 - ÉVALUATION DU PROGRAMME NATIONAL DE LUTTE CONTRE LE TABAGISME EN FRANCE (June 2023) Marion Devaux, Alexandra Aldea, Aliénor Lerouge, Marina Dorfmuller-Ciampi and Michele Cecchini- in French only, English version to be released soon,

NO. 154 - INNOVATIVE PROVIDERS' PAYMENT MODELS FOR PROMOTING VALUE-BASED HEALTH SYSTEMS (APRIL 2023), Luca Lindner and Luca Lorenzoni

NO. 153 - SOCIO-ECONOMIC AND ETHNIC HEALTH INEQUALITIES IN COVID-19 OUTCOMES ACROSS OECD COUNTRIES (MARCH 2023) Caroline Berchet, José Bijlholt and Mariko Ando

NO. 152 - IMPROVING THE TIMELINESS OF HEALTH EXPENDITURE TRACKING IN OECD AND LOW- AND MIDDLE-INCOME COUNTRIES (FEBRUARY 2023) Michael Mueller, Caroline Penn, Chris James, Luca Lorenzoni and David Morgan

Recent related OECD publications

HEALTH AT A GLANCE 2023 – OECD INDICATORS (NOVEMBER 2023)

PURCHASING FOR QUALITY CHRONIC CARE - SUMMARY REPORT (October 2023)

EMBRACING A ONE HEALTH FRAMEWORK TO FIGHT ANTIMICROBIAL RESISTANCE (September 2023)

OECD HEALTH STATISTICS (2023) – July 2023. Access all datasets in the 2023 online database via OECD Health Statistics 2023 - OECD

IMPROVING LONG-TERM CARE IN CROATIA (July 2023)

BEYOND APPLAUSE? IMPROVING WORKING CONDITIONS IN LONG-TERM CARE (June 2023)

READY FOR THE NEXT CRISIS? INVESTING IN HEALTH SYSTEM RESILIENCE (February 2023)

STEP UP! TACKLING THE BURDEN OF INSUFFICIENT PHYSICAL ACTIVITY IN EUROPE (February 2023)

HEALTH SYSTEM PERFORMANCE ASSESSMENT FRAMEWORK (HSPA) - Czech Republic (May 2023) and Estonia (June 2023)

INTEGRATING CARE TO PREVENT AND MANAGE CHRONIC DISEASES - BEST PRACTICES IN PUBLIC HEALTH (May 2023)

HEALTH AT A GLANCE: LATIN AMERICA AND THE CARIBBEAN 2023 (April 2023)

TIME FOR BETTER CARE AT THE END OF LIFE (February 2023)

THE COVID-19 PANDEMIC AND THE FUTURE OF TELEMEDICINE (January 2023)

EU COUNTRY CANCER PROFILES 2023 (February 2023)

HEALTH AT A GLANCE: EUROPE 2022 - STATE OF HEALTH IN THE EU CYCLE (December 2022)

EQUIPPING HEALTH WORKERS WITH THE RIGHT SKILLS: SKILLS ANTICIPATION IN THE HEALTH WORKFORCE (December 2022)

PRIMARY HEALTH CARE FOR RESILIENT HEALTH SYSTEMS IN LATIN AMERICA (December 2022)

HEALTH AT A GLANCE: ASIA/PACIFIC 2022 (November 2022)

PRIMARY HEALTH CARE FOR RESILIENT HEALTH SYSTEMS IN LATIN AMERICA (December 2022)

For a full list, consult the OECD health web page at http://www.oecd.org/health/
New **Health Brochure**