Addressing Future Cybersecurity Threats in Digital Health

Technical consultation on cybersecurity & privacy protection
12 – 14 December 2023
WHO Headquarters, Geneva, Switzerland | Salle T

Background

As countries increasingly deploy information technology for digital health transformation, there is a growing need for cybersecurity preparedness and strategy to ensure the confidentiality, integrity, and availability of current and future digital health systems. Increasing digitization of global and domestic public health systems has introduced new challenges in resource-constrained settings, including how to securely collect, store, and analyze digital health data. Increased investments in digital transformation of health systems have historically not been matched by investments to ensure privacy by design nor to strengthen, secure, and protect digital health systems from cyber threats. Concurrently, the frequency of cyberattacks perpetrated has increased, with governments and non-profits most frequently targeted. Cyber-attacks are increasingly targeted at low- and middle-income countries (LMICs), where lower cybersecurity preparedness increases vulnerability.

As part of the Global Strategy on Digital Health 2020 – 2025, Strategic Objective 3: Strengthen Governance of Digital Health at Global, Regional and National Levels, the proposed actions by the secretariat include the development of evidence-based technical guidance on privacy and security in the context of health systems strengthening, health emergency response and healthy wellbeing. Thus, World Health Organization (WHO) has drafted guidance to support Member States and key stakeholders to plan, budget, and implement cybersecurity and privacy protection in digital health interventions. The two guidance documents include a comprehensive guidance document on how to implement and invest in cybersecurity and privacy protection for digital health interventions that contain individual-level data, and a 10-pager toolkit that would provide an executive summary on cybersecurity and privacy protection for those planning and budgeting digital health interventions.

Further, WHO in collaboration with the U.S. Centers for Disease Control and Prevention (CDC) Global Health Center (GHC) seeks to obtain feedback on this guidance and identify strategies and mechanisms to strengthen the implementation of cybersecurity preparedness and resilience activities across resource-constrained settings. Through a co-sponsored technical consultation facilitated by Vital Wave, Inc., WHO and CDC will bring together key stakeholders in digital health, cybersecurity, and privacy protection. The consultation will provide an opportunity to assess the availability and applicability of existing cybersecurity best practices and take steps toward a strategic roadmap for addressing identified deficiencies or barriers towards achieving implementation of holistic cybersecurity preparedness and resilience.

Workshop Objectives

1. Collectively articulate the nature and magnitude of the gap between the current state of cybersecurity preparedness in resource-constrained settings and the desired future state.

2. Begin drafting a collective roadmap to address identified gaps and increase resiliency of digital health systems and implementations against cyberthreats over a timeline of 5-10 years

3. Review and provide feedback on drafted cybersecurity and privacy protection guidance being developed by WHO.

Anticipated Outcomes

- Common understanding of the current state of cybersecurity and privacy protection policy in resource-constrained environments, including identification of drivers of, or barriers to, the current state of cybersecurity preparedness

- Identification of priority areas for inclusion in a collective roadmap, which may include addressing gaps with respect to fit-for-context resources, political support for funding cybersecurity programs, data availability, implementation support, human resource availability and technical capacity, and other areas identified through the consultation.

- Documented gaps and dependencies between current state and the desired future state of cybersecurity and privacy protection

- Clearly articulated actions and realistic outcomes to be achieved in 5-10 years to fill identified gaps

Workshop Approach

The workshop will explore real-world case studies, the state of cybersecurity assets, and needed investments to close the gap in cybersecurity preparedness and resilience in resource-constrained settings. The event will include approximately 30 representatives including technical cybersecurity and digital health experts from government, parastatal, academic, and private sector stakeholders. The consultation is planned for 12 – 14 December at the WHO headquarters in Geneva, Switzerland.

The consultation will provide an opportunity for attendees to:

- Articulate the magnitude of the gap between the current state of cybersecurity capacity and the necessary future state to protect against cyberthreats.

- Holistically map key contributors to success including human capacity, legal frameworks, technical infrastructure and tools.

- Identify concrete and actionable approaches to realizing effective cybersecurity in digital health, building off of existing and emerging technical guidance.

- Collaboratively identify and articulate the issues faced, including proposed actions needed to address the identified gaps or barriers to achieving cybersecurity preparedness and resilience in digital health systems in resource-constrained environments.

Ultimately, this event will be a step towards increasing global cyber readiness as digital health solutions are proliferated globally.

Provisional List of Participants

- Cybersecurity and privacy protection technical experts from: Ministries of health, Ministries of ICT, Academia, and Private sector technology companies
- Global digital health implementers and experts with experience in country
- Key donors and funders of digital health implementations in countries
- WHO secretariat

Provisional Agenda

	12 December	13 December	14 December
Overall Goal	**Day 1: Understand the current state of cybersecurity and challenges to implementing cybersecurity programs in digital health contexts**	**Day 2: Articulate the gap between the current and desired state of cybersecurity preparedness**	**Day 3: Map next steps to fill gaps**
Morning Session 1 9:00am – 10:30am	Framing the problem	Identifying the desired state for digital health systems in low-resource settings	Identifying technical needs and cyber preparedness goals to fill identified gaps
Coffee Break 10:30am			
Morning Session 2 11:00am – 12:30pm	Presentation of real-world case studies	Exploring strengths and limitations of current cybersecurity resources and approaches	Continued: Articulating needs and goals
Lunch 12:30pm			
Afternoon Session 1 1:30pm-3:00pm	Contextualizing cybersecurity for low-resourced health systems	Analyzing gaps between the current state and desired state of cybersecurity preparedness	Mapping dependencies and opportunities to advance goals
Coffee Break 3:00pm			
Afternoon Session 2 3:30pm-5:00pm	Identifying drivers of the current state of cybersecurity preparedness	Continued: Analyzing gaps between current-state and desired state of cybersecurity preparedness	Documenting next steps
End of Day 5:00pm			