COMMITTEE: World Health Assembly (WHA)

QUESTION OF: Addressing the safety concerns of technology and artificial intelligence implementation in healthcare services

MAIN SUBMITTER: China

CO-SUBMITTERS: Bulgaria, Colombia, Czech Republic, Germany, Hungary

THE WORLD HEALTH ASSEMBLY,

Recognizing the increasing reliance on digital technologies, including electronic health records, telemedicine, and AI-driven systems in healthcare, which makes healthcare infrastructures highly vulnerable to cyberattacks,

Alarmed by the rise in hacking incidents targeting healthcare systems globally, including ransomware attacks on hospitals, breaches of sensitive patient data, and the potential for life-threatening disruptions to healthcare services,

Acknowledging that many healthcare organizations, particularly in Less Economically Developed Countries (LEDCs), lack the technical expertise, financial resources, and infrastructure necessary to defend against cyber threats,

Recalling prior international agreements and resolutions emphasizing the importance of data security, privacy, and international cooperation,

1. Urges member states to adopt a Global Healthcare Cybersecurity Framework (GHCF) to enhance the security of healthcare systems and safeguard against hacking in collaboration with World Health Organization (WHO) and International Telecommunication Union (ITU) for means such as but not limited to:
    a. strengthening cyber security infrastructure by:
        i. mandating the use of advanced encryption technologies for storing and transmitting sensitive patient data, including electronic health records and telecommunications
        ii. requiring all medical devices connected to hospital networks such as imaging systems and diagnostic tools to undergo cybersecurity certification including the CompTIA Security which is recognized by the

relevant governments such as the U.S. Department of Defense before deployment

iii. ensuring regular updates and patching of software in all healthcare IT systems to eliminate vulnerabilities exploited by hackers

iv. establishing secure backup systems to protect critical data and enable rapid recovery in the event of attacks

b. building cybersecurity workforce capacity by:

i. creating national training programs for healthcare IT staff to detect and respond to cyber threats effectively by informing these threats within 72 hours but resolving such issues within 69 days under the ITU

ii. offering scholarships and grants with government funding to incentivize people in training into cybersecurity specialist, particularly in Less Economically Developed Countries (LEDCs)

iii. developing public-private partnerships to share expertise and train healthcare administrators on best practices for cybersecurity

c. promoting international collaboration to address various aspects of cyber threats through means such as but not limited to:

i. establishing a WHO-led Global Healthcare Cybersecurity Task Force to coordinate international efforts to combat cyber threats targeting healthcare systems

ii. holding bi-annual meetings between nations regarding emerging cyber threats and vulnerabilities through a centralized global database that is analyzed by experts' data analysis from WHO

iii. encouraging cross-border agreements to criminalize healthcare hacking activities, prosecute offenders, and disrupt networks of cybercriminals

iv. providing technical and financial assistance to LEDCs to strengthen their healthcare cybersecurity capabilities by creating a dedicated fund under the WHO or World Bank;

2. Further urges the establishment of a Global Task Force that focuses on healthcare technology and safe and precise use of AI to develop standards that are globally agreed on in ways such as but not limited to:

a. developing comprehensive guidelines and best practices for the safe and ethical implementation of AI technology in healthcare by:

i. setting standards for data privacy and security to protect sensitive patient information from unauthorized access and breaches

ii. putting in place thorough procedures to verify and test AI algorithms and medical devices to guarantee their precision, dependability, and safety prior to being used in clinical settings

        iii. recommending for the integration of human oversight and accountability mechanisms where humans will be monitoring the AI-driven healthcare systems to prevent over-reliance on these technologies and ensure more responsible decision-making, prioritizing patients' safety

b. facilitating international collaboration for knowledge sharing among member states, technology developers, health care providers and other relevant stakeholders to discuss common safety challenges and promote the development of globally harmonized safety frameworks by:
    i. encouraging biannual meetings of different stakeholders to engage in regular dialogue and exchange of information, fostering an environment where diverse perspectives can be integrated into the development of the criteria and understanding of a unified safety measure
    ii. arranging online meetings and collaborative projects that unite experts from various countries to discuss successful approaches to safety challenges and best practices regarding the use of AI in healthcare

c. conducting regular assessments on a semi-annual basis regarding the safety landscape in healthcare technology, identifying the emerging risks and providing updates to the WHO and its member states by:
    i. setting up secure, anonymous systems for reporting unethical practices, ensuring accessibility and protection for whistleblowers
    ii. allowing data scientists to analyze the collected data to detect trends and patterns regarding the safety issues and share with different member states to be published for the public to access
    iii. getting insights from healthcare professionals regarding how patients would be impacted by these trends, enabling the WHO to effectively prioritize certain safety initiatives

d. allowing the government to establish punitive measures for violations of AI regulations in healthcare through means such as but not limited to:
    i. classifying violations into categories based on severity, with minor infraction receiving warning and sent to training, moderate ones facing substantial fines and audits, and severe offense leading to license revocation and potential criminal charges decided on an ease to case basis
    ii. imposing financial penalties, proportional to the severity of the violation, to deter non-compliance and fund ethical AI initiatives
    iii. enforcing temporary or permanent suspension of AI system certifications or licenses
    iv. ensuring accountability through criminal liability, with penalties such as imprisonment or fines for deliberate misuse causing significant harm

e. improving AI driven decision-making process by integrating safeguards such as but not limited to:

i. establishing human-in-the-loop (HITL) protocols to ensure human oversight in critical healthcare decisions and to override AI recommendations when necessary

ii. promoting transparency by requiring AI systems to disclose when and how decisions are influenced by algorithms in language that is accessible to patients

iii. creating feedback systems for patients and healthcare providers to report concerns or errors stemming from AI-driven decisions;

3. Calls upon Member States to develop a global program called the AI Healthcare Equity Program (AIEP) to address challenges in training, access, and ethical implementation of AI technology used in healthcare, through means such as but not limited to:

a. collaborating with AI Healthcare companies who have shown to produce reliable and safe technology from the past three years and are recognized by relevant committees and councils to conduct globally recognized training and certification programs through means such as but not limited to:

i. creating standardized, multilingual training modules on the effective use of AI and IT systems in healthcare especially by providing slide presentations, videos, and guides both in paper and electronic format

ii. providing workshops and conferences through partnerships with NGOs and private-sector technology developers including both informative lectures and interactive activities related to AI literacy and IT developments

iii. ensuring that all information created covers the ethical use of AI in healthcare including both the General Data Protection Regulation (GDPR) and similar laws like the Genetic Information Non-discrimination Acts (GINA)

iv. putting in place a comprehensive training program that covers risk assessment, data privacy, AI ethics, and safety measures

v. providing access to resources for universities integrating AI education in their medical programs

b. improving the access of AI and IT infrastructure in less economically developed countries (LEDCs) through means such as but not limited to:

i. creating an international funding mechanism supported by WHO and donor nations to subsidize the purchase of AI tools and IT equipment for LEDCs

ii. fostering partnerships between developed nations and LEDCs to share expertise, equipment, and technology

iii. promoting the development and adoption of reliable AI platforms, outlined by the AIEP and tools to minimize licensing cost and enhance accessibility, for LEDC healthcare providers

c. supporting collaboration among governments, private companies, and international organizations to create affordable and scalable AI healthcare solutions specialized for LEDCs through means such as but not limited to:

i. developing scalable pilot programs in LEDCs to test and refine AI healthcare solutions tailored to address local health challenges, with insights from relevant international organizations applied to enhance effectiveness and adaptability

ii. facilitating public-private partnerships (PPPs) to encourage investment in AI healthcare solutions for LEDCs, including financial incentives such as grants and co-development opportunities with private companies

iii. promoting collaborative data-sharing frameworks to improve the cultural and demographic relevance of AI tools while adhering to global data protection laws such as the GDPR and Health Insurance Portability and Accountability Act (HIPAA);

4. Encourages collaboration to address issues regarding healthcare technology through international partnerships, data-sharing agreements, and joint research initiatives to improve AI-based healthcare solutions in ways such as but not limited to:

a. offering incentives for collaborative research that are aiming to improve the safety of AI technologies used in healthcare by:

i. allocating funds and resources to support research projects that work to create safer and more effective AI solutions meeting the Global Regulatory Framework for AI in healthcare by bringing together a range of experts in this field and healthcare institutions

ii. establishing recognition programs that publicly acknowledge and reward institutions or researchers who make substantial contributions to improve the safety of AI in healthcare

b. encouraging collaboration to advance innovation and address safety issues in healthcare AI technology through:

i. promoting collaboration between member states creating a collective database including experience about healthcare technology and AI safety, with a focus on collaboration between countries with varying levels of technological development

ii. forming public-private partnerships, such as those with private businesses and government organizations, to combine resources and expertise for collaborative research projects aimed at tackling important safety issues in healthcare AI technology;

5. Suggesting member nations to increase public understanding on the importance of safe technology and artificial intelligence in healthcare services in ways such as but not limited to:

a. developing educational campaigns that can be implemented to increase public understanding of the importance of safety in healthcare technology by:

i. creating social media content to inform the public about healthcare technology safety concerns and steps they can take to protect themselves

ii. displaying short and concise posters on the topic of AI safety and the different healthcare technologies that are currently available in public areas as well as incorporating digital and physical versions on social media platforms, official healthcare websites, poster boards around the hospital and healthcare applications to maximize public awareness

iii. distributing information packets to individuals living in LEDC countries to ensure that they are informed regarding the existing AI technologies in healthcare services and the importance of safety for these technologies

iv. encouraging healthcare professionals and technology specialists to participate in various events concerning both professional suggestions and public opinions about AI healthcare technology

b. utilizing media influence to promote policymaking and for more efficient regulation of the industry in ways such as but not limited to:

i. conveying the latest research findings and public demands in healthcare technology and AI to policymakers through media channels, aiming to revise and provide stronger policies

ii. exposing unsafe and non-compliant products and services through media, encouraging companies to strengthen self-discipline and adhere to the safety protocols and standards set by the industry, while fostering greater connectivity with LEDCs to ensure access to safe and compliant healthcare technologies.