Twelfth Pacific Health Ministers Meeting
August 28-30, 2017

World Health Organization
Western Pacific Region

TE MARAE ORA
COOK ISLANDS Ministry of Health

Pacific Community
Communauté du Pacifique

TWELFTH PACIFIC HEALTH MINISTERS MEETING **PIC12/INF_1**

Rarotonga, Cook Islands
28–30 August 2017

16 August 2017

ORIGINAL: ENGLISH

Information document:
Cybersecurity and its implications for health information systems

Cybersecurity is a core component of health information system (HIS) development. A more secure Internet environment and better-protected information privacy improve information sharing and use in a well-functioning HIS.

Digitized information provides support to health-related decision-making at all levels of health systems, including in mobilizing community support, planning clinical services, facilitating special consultations, organizing effective health promotion activities, and supporting national health policy development. A variety of electronic tools are utilized: community maps, civil registration databases, electronic medical records, long-distance consultation assistant systems (such as telemedicine, etc.), health research records and health information platforms.

Important dimensions to improve cybersecurity and information privacy

Cybersecurity involves two areas in HIS: improving Internet security to avoid cyberattacks, preventing the disruption of routine health facility business, protecting key information and managing web-based information or health related services to protect health-related information; and improving cybersecurity to protect information privacy.

In most countries, health system cybersecurity is directly related to general Internet security regulations and practices. It is also linked to regulations relating to health information and communication technology (such as how information generated through medical devices is transferred, stored and protected, who is responsible and who should own information thus generated).

Clearly defined roles and responsibilities of parties involved in health-related information, normally through local or national legislation, are critical to establishing a foundation for cybersecurity in HIS. Actions to improve cybersecurity require multiple stakeholders and efforts and actions across several sectors. The health sector needs to engage with national Internet security authorities, manufactures, information and communication technology providers, hospitals, and health service providers to define appropriate approaches and actions to improve cybersecurity and information privacy. A strong governance mechanism is needed to ensure that all segments of health systems adhere to minimum cybersecurity requirements and take necessary action to protect information privacy to avoid the misuse of health information.

Throughout this process, detailed technical guidance and operational procedures must be introduced and applied in health systems, including well-defined processes for information collection and sharing. This includes determining what information should be collected at a health facility, who should access individual information, what information should be transferred as a result of information requests, how such information should be processed and stored, what level of di-individualizing information collection and storage according to the purpose of information utilization, who can access the aggregated information, what level of Internet security arrangements should be introduced to improve cybersecurity in different computer systems, etc.

Current cybersecurity environment

Since global ransomware attacks have become more frequent, a best-practice cybersecurity approach for critical services such as hospitals and other health facilities is needed. The importance of a layered approach to HIS security is essential as there is no single solution that can protect them in an environment where data is freely exchanged, and where health staff utilize equipment connected to a multitude of networks, many of which are unprotected.

Information Technology Security Standard ISO/IEC 27000

There are a number of widely available international standards and national data legislation examples that art applicable to all sectors, including government and public health, which can help mitigate the inherent risks in operating in a connected environment. These can be implemented in any industry and in any size organization, allowing them to provide robust information security management for connected hospitals, clinics and HIS.

Of these, the International Standards Organization (ISO) 27000 series,[1] commonly known as ISO27K, is the most prominent. This series underlines best practices in the field of information security, and provides recommendations to manage risks through security controls, bolstering the overall information security management process. As the series provides guidance and checklists, it can be implemented by both small and large entities.

System Planning and Design

There is no quick fix to address cybersecurity threats. Information technology security system implementation needs to take a layered approach, addressing risks associated with people, processes and technology, and taking into account the multiple stages of a cyberattack; targeting a facility, compromising a system, and finally breaching and controlling it.

[1] https://www.iso.org/isoiec-27001-information-security.html

The stages and layers of a cybersecurity threat highlight opportunities where health information technology systems can be secured. Technologies exist that can prevent or limit exposure at each level. These include security patches, anti-malware software, and next generation firewalls and intrusion prevention systems to protect the overall network.

The key to a layered, secured approach is designing effective HIS technology. This does not need to be a costly endeavour as the open source community provides many of the required IT tools at little to no cost, although long-term hardware and other support costs need to be factored in.

Planning in terms of the critical control objectives highlighted in the ISO27K standard and national data-related legislation is important. A few potential security measures include:

- Installing timely security patches and software updates on medical devices, health IT systems, and connected networks to defend against potential compromise of systems
- Securing information systems and other devices through encryption
- Selecting software that complies with international security standards and is frequently updated and maintained by the manufacturer
- Segregating networks, specifically medical devices and those that contain sensitive information, from the rest of the health facility to limit exposure to network-based attacks
- Implementing information technology security systems at the layers exposed to attacks
- Implementing resilient back-up, restoration, and business continuity procedures

Many of the IT components of the layered security approach are also available today on the “cloud”, either through software as a service (SaaS) or other forms. Within the limits of connectivity and national legislation on privacy and encryption of patient and health systems data, a cloud-based approach to cybersecurity provides significant returns by integrating health facilities that are not physically connected. This approach also addresses the shortage of qualified information security staff, who are not normally available at health facilities located in remote locations, through outsourced or centralized IT services.

Common implementation challenges and possible actions from countries

HIS are quite diverse from an infrastructure perspective, in terms of scope of services, and in technical capacities, as they include large complex hospitals and single practitioners. This diversity poses challenges in allocating responsibility, supervision, and cybersecurity measures across systems. Lack of resources and technical capacity in health facilities, difficulty in keeping up-to-date with advances in technologies and threats, capacity to act on information security threats, and a general lack of knowledge and awareness of cybersecurity among health workers, are common challenges for improving cybersecurity in the health sector.

Some actions that might be considered for countries to improve their cybersecurity include:

1. Clearly defining and streamlining cybersecurity leadership, responsibility, governance mechanisms, and expectations for health system.
2. Increasing the security measures and resilience of medical devices and health IT equipment.
3. Developing and improving health care workforce capacity to ensure cybersecurity awareness and technical capacities in health systems.

4. Identifying mechanisms to protect research and development efforts and intellectual property from attacks.
5. Improving information sharing related to cybersecurity threats, weaknesses and mitigation efforts across health systems.

References:

Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington, DC: Institute of Medicine, The National Academies Press; 2009 (https://doi.org/10.17226/12458, accessed 8 August 2017).

Report on improving cybersecurity in the health care industry [pdf], Washington, DC: US Department of Health and Human Services, Health Care Industry Cybersecurity Task Force; June 2017 (https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf, accessed 8 August 2017).