Kenya Healthcare Federation
The Health Sector Board of KEPSA

Position Paper on Cybersecurity Standards for Networked Medical Devices

INTRODUCTION

Hospital management information systems and the Internet of Things (IoT), Networked medical devices such as patient monitors, infusion pumps, and imaging systems have become integral to healthcare delivery around the world. However, legacy equipment and subsequent enhanced connectivity have increased the surface area for cybersecurity threats that could endanger patient safety. Recent research indicates that health information systems and medical devices have become frequent targets for cybercriminals seeking to access protected health information or disrupt hospital operations.

In Kenya, the uptake of connected medical technology has rapidly accelerated in recent years. However, cybersecurity precautions have often not kept pace. There is an urgent need to implement adequate safeguards to match the risks that come with networked health information systems. It is worth noting in the 31st Cyber threat report by the Communication Authority of Kenya, web application attacks rose by 36% in one quarter.

This paper lays out the position of the Kenya Healthcare Federation (KHF) on adopting consistent cybersecurity standards for networked health systems used in Kenyan healthcare facilities, whether in the public or private sector. The KHF represents over 300 private and faith-based healthcare providers in the country.

CHALLENGES OF CONNECTED DEVICES

Connected health systems offer substantial benefits, including remote monitoring of patient vitals, alerts sent to caregivers, and software/firmware updates to fix bugs and add new capabilities. However, cybercriminals can potentially exploit vulnerabilities to:

- Access confidential patient health records stored on or transmitted by the device.
- Manipulate device functions leading to incorrect outputs or dosage amounts.
- Use the device as an entry point to access wider hospital networks and systems.
- Hold hospital systems for ransom by locking access or disabling functionality.

These risks are heightened due to the growth of the Internet of Medical Things (IoMT), as more monitoring devices and wearables connect to hospital networks. In addition, many legacy medical devices run outdated operating systems that are highly vulnerable to attacks.

REGULATORY GUIDELINES

Kenya lacks comprehensive regulations focused specifically on cybersecurity for networked medical devices. However, there are relevant requirements contained in broader laws and standards, including:

- The Kenya Information and Communications Act 1998 provides standards applicable to electronic devices and online systems.
- ISO 27799 guidelines adopted in Kenya establish optimal security practices for health information systems.
- The Health Information Systems Policy 2016 speaks to protecting patient data privacy.

While these regulations relate to cybersecurity controls, they lack specific directives tailored for networked medical devices. Prescriptive guidance is necessary for hospitals and vendors seeking to secure this specialized category of connected technology.

KHF RECOMMENDATIONS

To address these gaps, KHF puts forward the following recommendations:

1. Establish national baseline cybersecurity standards for the procurement of networked health systems in Kenya. This should cover areas like device authentication, access controls, vulnerability reporting and coordinated disclosure, encrypted storage and transmission, and other technical specifications.
2. Require vendors of networked hospital systems to notify healthcare providers about cyber vulnerabilities identified in their equipment or systems. Vendors should issue fixes and security patches in a timely manner.
3. Set up a medical device vulnerability coordinating body to help vendors disclose flaws securely and enable hospitals to address issues across different devices. This can be developed on existing platforms like the Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC).
4. Incorporate medical device cybersecurity into continuous education and training programs for hospital IT, biomedical engineering, clinical engineering, and technology planning staff. This will spur the adoption of secure device lifecycle management practices.
5. Encourage hospitals to conduct regular cyber risk assessments focused specifically on networked medical technology. This should cover risk analysis, device inventory mapping, vulnerability scanning, and contingency planning.

By enacting clear standards and facilitating education on medical device security, Kenya can harness connectivity in healthcare while safeguarding patient well-being, data integrity, and continuity of care. The KHF and its members stand ready to support efforts by policymakers and regulators to enhance protections for networked hospital technology.

Kenya Healthcare Federation

Position Paper on Cybersecurity Standards for Networked Medical Devices

KHF Digital Health Committee