HealthManagement
Promoting Management and Leadership

Cybersecurity and Privacy Best Practices for Medical Practitioners

John Walubengo
******@***mmu.ac.ke

ICT Lecturer - Multimedia
University of Kenya
Nairobi, Kenya

Many private practitioners are deploying information systems in their private medical facilities to take care of various processes such as patient on-boarding, patient record keeping, patient accounts amongst others. However, there is less effort to ensure that these information systems have the necessary controls to safeguard patients records and meet good privacy and security practices. This article looks at some of the risks, challenges and their safeguarding measures.

Key Points

- This article targets the smaller, private medical practitioner who is increasingly having to navigate and rely on ICTs in their daily medical practice.
- The article addresses the common daily ICT risks that such private medical practitioners may face and how they can mitigate them.

Cybersecurity, Data Privacy

Many larger medical facilities such as mid-sized and above hospitals already employ a comprehensive team of in-house ICT professionals to handle their cybersecurity and data privacy concerns. We therefore assume those types of medical facilities already have their concerns taken care of under ICT professionals.

This article therefore targets the smaller, private medical practitioner who is likewise having to rely on ICTs in their daily medical practice - while not having the budgets or availability for hiring in in-house ICT Professional.

What are the typical ICT risks that such private medical practitioners face and how can they mitigate them?

Firstly, there is the admission process. Many private practitioners have a simple database for onboarding their patients. Whether it's as simple as a worksheet operated by the receptionist or a more sophisticate version hosted on a computer or even in the cloud, the information security concerns remain the same.

Some of these concerns include whether access controls are sufficient to limit un-authorised access to the patient contacts database. Restrictions to patients' contacts details is now one of the provisions in most data protection/privacy regulations across the globe since many third-party health providers such as pharmacist, insurers amongst others would want to harvest such a contact list in order to start marketing all manner of products to un-suspecting patients.

Once the patient has been admitted, a patient file has now been created outlining the personal medical history of the patient as they move across from triage, through consultation, treatment and finally pharmacy stages. Many private practitioners have automated these stages as well and would face the common info-security risks known as the CIA triad – Confidentiality, Integrity, and Availability risks.

Confidentiality is about putting in place controls to ensure that only authorised personnel can access the patient records. More importantly, one must have granular levels of authorised access such that the accountant has no reason to see the full-blown patient history as seen by the

medical practitioners.

Integrity is about putting in place controls to ensure that only authorised medical practitioners can update the patients' medical history. Additional controls should be in place to ensure that such updates are not made in error or mixed up between different patients since such could lead to serious implications in terms of medical prescriptions and others.

Finally, *Availability* is about putting in place controls to ensure that the information system can provide service as and when it is needed – essentially be available on a 24x7 basis. Failure to regular servicing of the computer hardware and software may lead non-availability of service when the hardware malfunctions during a busy period at the medical facility.

Similarly, the recent ransom attacks, where patient records are encrypted by hackers until they are paid up to release the decryption keys, is another example of threats against the Availability principle.

To mitigate against the CIA risks, the following would be required.

Minimising *confidentiality* risks, one must have a reliable IAM (Identity & Access Management) system which basically issues login credentials to authorised personnel to access various aspects of the information system at granular levels, based on their job description.

Minimising *Integrity* risks, the information system should have an audit trail that can regularly be reviewed to see what actions or updates happened on a patient record, by when they happened, by whom and if they were legitimate.

Finally, to minimise *Availability* risks, the data on the information system should regularly be backed up in a remote location to ensure that the medical facility can be able to recover and restore patient data in the event of a disaster or a ransomware attack.

Conflict of Interest

None

Published on : Fri, 15 Sep 2023