The Queens Medical Centre is a community clinic that has opted to implement a web-based appointment and scheduling management information system (ASMIS). This system enables online booking of appointments by collecting the patient's vital information so as to determine which specialist is best to attend to a given case. Even though some of the benefits of ASMIS are:

- the residents will be getting access to care on time,
- the clinic will be able to respond to the rate of growth of the community population and
- the ASMIS system is well secured from cyberattacks,

human factors need to be prioritised to ensure achievement of ASMIS' security, usability and functionality.

The 3 human factors that are to be addressed include:

1. **Lack of Cybersecurity Awareness:**

   Cybersecurity awareness is one of the major human factors to be considered when implementing ASMIS. This is because when users have very little to none cybersecurity knowledge, they will not know how to avoid, identify and handle cyberattacks (Nifakos , et al., 2021). Therefore, they might perform more human errors plus become more prone to cyber-attacks like phishing, data breaches, etc. Moreover, sometimes users are ignorant or do not put enough effort into learning, applying and following cybersecurity knowledge and practices.

So, with the use of seminars, videos, documents, questionnaires, etc, both the patients and staff may be trained on cybersecurity (risks, vulnerabilities, benefits and mitigations) and also on how to use ASMIS more effectively efficiently and safely.

2. **Fatigue/Tiredness:**

The successful implementation of ASMIS may be hindered by users' fatigue. As users been humans, they can be susceptible to tiredness that might lead to an increase of human errors and loss of attentiveness. (The CERT Insider Threat Team, 2013)

Fatigue may be contributed by:

- Mental and physical work overload on users (The CERT Insider Threat Team, 2013)
- Nested processes that need to be executed for a function or task to be performed.
- A lot of security features that causes users (especially users with disabilities or short-term memories) to be frustrated and fatigued while performing them. E.g., use of very complex passwords and pins, changing passwords after a short period of time (like every 2 weeks), nested MFAs and CAPTCHAs that needs to be done and validated, etc. (Sasse & Rashid, 2019)
- A lot of errors that arise and slow runtime when users use the system that leads to frustration and fatigue.

This can be mitigated by practising better management i.e., more selfcare and less stress.

3. **Lack of User Adaptation and Acceptance**

When users do not embrace or accept ASMIS, the implementation of ASMIS in the clinic will have a higher chance of been unsuccessful. Some of the factors that can lead to this are:

- Poor or complicated user interface structures and system management that confuses and frustrates users.
- User's lack of training about the system and its benefits, and how to use it (Its functionality).
- Users have a lack of trust and are not confident enough about ASMIS and its technology.
- User's emotions (are they eager and happy with the ASMIS or they are sad or angry about it) and the pressure the users undergo while using ASMIS.
- Lack of transparency whereby users and patients are less aware of how their information will be handled once they give it out.
- User limitations and dissatisfaction with the features offered by ASMIS e.g., system inaccessibility and user unfriendliness. (Sasse & Rashid, 2019)
- Lack of ways patients and staff can provide feedbacks about the system or ask for technical help. (Venkatesh, et al., 2003)
- Inaccessibility and minimum ease of access and use to all users including users with disabilities

The success of ASMIS will largely depend on the ability of patients and staff to become familiar with and adjust to ASMIS as well as be willing to use it effectively. This can be achieved by focusing on the ease of access and use (easy and clear user interface design, etc) of ASMIS, user training and giving of feedback.

In conclusion, the deployment of ASMIS at the Queens Medical Centre has the potential to bring numerous benefits to both the clinic and the community. However, efficiency, security and success of ASMIS is greatly dependent on the prioritization of human factors such as cybersecurity awareness, fatigue/tiredness, and lack of user adaptation and acceptance.

Therefore, it is crucial to address and ensure these human factors are taken into consideration during the implementation of ASMIS so as to guarantee optimal functionality, usability and security.

References

Nifakos , S. et al., 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors,* 21(15), p. 5119.

Sasse, A. & Rashid, A., 2019. *Human Factors Knowledge Area.* [Online]
Available at: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf
[Accessed 04 February 2023].

The CERT Insider Threat Team, 2013. *Unintentional Insider Threats: A Foundational Study.* [Online]
Available at: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf
[Accessed 04 February 2023].

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D., 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* 27(3), pp. 425-478.