



According to a post in the August 2017 issue of the SolutionReach blog, the author mentioned that the average phone call to schedule an appointment takes over eight minutes. Multiply that by the number of appointments scheduled each day and your practice may be spending hours on appointment scheduling on a daily basis.

Since Queens Medical Care is implementing a web-based application for ASMIS we should consider the human factors and look for their solutions.

The three identified human factors which could breach

the ASMIS of Queens' Medical Care are as per below:

THE HUMAN FACTORS

1. Schedule appointments on a flexible basis
2. Patients must be correctly triaged and risk categorized.
3. Staffs accessing phishing emails



1. SCHEDULE APPOINTMENTS ON A FLEXIBLE BASIS

Problems in ASMIS:

- Lacks flexibility in medical setting
- Cannot handle cases not defined
- Example: New-born caring appointment



Human Factor Related to Problem:

- ☐ Users abuse the system by tampering with data

Source: Improving Access to Healthcare with Online Medical Appointment System, 2019

3



A real-time web-based appointment and scheduling management information system (ASMIS) lacks flexibility in the medical setting because the automatic appointment systems are not intelligent enough to handle cases not predefined for example, in the case of the new-born caring. Therefore, users abuse the system by tampering with data while trying to schedule their appointment (Improving Access to Healthcare with Online Medical Appointment System, 2019).

1. SCHEDULE APPOINTMENTS ON A FLEXIBLE BASIS

Proposed solution

Use Control Relocation and Artificial Intelligence (AI)

- Patients self-schedule appointment
- No restriction to business hours
- Allows real-time booking
- AI suggests non-predefined instances



Source: 6 Ways to Schedule Patients Effectively and Efficiently, 2017, Thibodeau, 2018

4



While trying to make the ASMIS flexible, Queens Medical Care can implement a control relocation system along with an AI algorithm to handle cases that are not pre-defined.

With the control relocation, patients self-schedule their appointment and take control over which doctor and the time for the appointment. It improves flexibility for the patient as they can make an appointment online without restricting to business hours. It also improved patient satisfaction and

allows real-time booking. (6 Ways to Schedule Patients Effectively and Efficiently, 2017).

Studies have revealed that the majority of patients prefer to schedule their own appointments online. On the other hand, artificial intelligence, the AI, will adjust its calculations and suggests non-predefined instances much faster than a human could, exploring millions of possibilities practically instantaneously. Thus, the more complex the reality of a hospital or medical clinic, with more varied types of medical appointments and physician specialists; the more artificial intelligence saves time and optimizes schedules (Thibodeau, 2018).

2. PATIENTS MUST BE CORRECTLY TRIAGED AND RISK CATEGORISED

Problems in ASMIS:

- Patients use ASMIS for non-emergency situations.
- Doctors skip urgent appointments

Human Factor Related to Problem:

- Users misinterpret emergency conditions

Source: Web-Based Medical Appointment Systems: A Systematic Review, 2017

5



It is challenging to sort patients who made appointments through real-time Web-based appointment systems. Patients may use ASMIS for non-emergency situations that does not need to be handled immediately by an emergency room or urgent care. As a result, doctors skip urgent appointments. Since schedulers are no longer involved in the appointment process, the systems should be capable of sorting patients and classifying their risks accurately (Web-Based Medical Appointment Systems: A Systematic Review, 2017).

2. PATIENTS MUST BE CORRECTLY TRIAGED AND RISK CATEGORISED

Proposed solution

Use Principle of Least Privilege (PoLP)

- Provide minimum access to ASMIS users
- Includes a critical step in safeguarding privileged access



Source: Least Privilege, 2021

6

When it comes to securing data access, using the concept of least privilege is the most straightforward and reliable option.

It is a notion in information security that states that a person should only be granted access to the resources they require to complete a task. In the case of Queens' Medical Care ASMIS, we should provide minimum access to ASMIS users while using the system to avoid the abuse of Web-based appointment systems for problems that do not require rapid attention. Most cyber security experts

agree that the concept of least privilege is a good one to follow since it includes a critical step in safeguarding privileged access (Least Privilege, 2021a).

2. PATIENTS MUST BE CORRECTLY TRIAGED AND RISK CATEGORISED

Why is PoLP important?

1. Reduces offensive area of cyber attacks
2. Enhances the efficiency of end-users
3. Automatically reset all administrators' passwords after each usage

Source: Least Privilege, 2021

7



- It reduces offensive area of cyber-attacks. Today, even accidental assaults rely on credential exploitation. In order to decrease the attack surface, least privilege enforcement restricts access to super-user and administrator functions.
- It enhances the efficiency of end-users. In this way, users of the Queens Medical Care system can assist minimize risk by eliminating internal administrator privileges
- It automatically resets all administrators' passwords

after each usage to negate any passwords that might have been recorded by keylogging software and to reduce the possibility of a Pass-the-Hash attack.

(Least Privilege, 2021b).

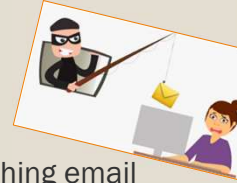
3. STAFFS ACCESSING PHISHING EMAILS

Problems in ASMIS:

- 24% of doctors could not spot a phishing email
- Privileged accounts are vulnerable

Human Factor Related to Problem:

- ☐ Due of fatigue and distraction, users open phishing emails.



Source: Garska, 2018, The Human Factor: The Hidden Problem of Cybersecurity - CYDEF, 2021


8

According to a post in the August 2018 issue of the IdentityAutomation blog, Katheleen Garska wrote that in the study, researchers found that 24% of doctors could not identify a phishing email, a number three times higher than non-physicians (Garska, 2018). During an attack, the privileged accounts are the most vulnerable.

Due of fatigue and distraction, users open phishing emails at some point during the working week. (The Human Factor: The Hidden Problem of

Cybersecurity - CYDEF, 2021)

3. STAFFS ACCESSING PHISHING EMAILS



Proposed solution

Improve the knowledge of the employees

- Regularly remind employees of risky behaviours
- Instruct employees on differentiating between genuine and fraudulent emails

Source: The Human Factor: The Hidden Problem of Cybersecurity - CYDEF, 2021

9

Cyber security specialists, too, use strong firewalls and other defences, but the human aspect is still a vulnerable element. To minimise human error for the phishing email case in Queens' Medical Care ASMIS,

- The administrators need to regularly remind employees of risky behaviours. Everything from downloading unauthorized software and using infected devices to visiting dangerous websites and generating weak passwords might be included in this.
- Instruct employees on differentiating between

genuine and fraudulent emails so that individuals may stay safe from phishing attempts. In addition, training should be updated or customized on a regular basis for various staff groups.

(The Human Factor: The Hidden Problem of Cybersecurity - CYDEF, 2021)

CONCLUSION

When it comes to anticipating, mitigating, and resolving human factors issues, refining and creating linkages and considerations should be the focus of future effort.



Source: Ferro, 2019

10



As a result of this discussion, it is clear that e-health presents a great potential for threat modelling, which may assist in identifying behaviours that could threaten the security of patient data. For example, we may utilize this information to create initiatives to minimize stress, workplace norms, lack of understanding, and so on, and anticipate the possibility of when human factors may influence a system's security. As a result, when it comes to anticipating, mitigating, and resolving human factors issues, refining and creating linkages and considerations should be the focus of future effort. (Ferro, 2019).

SOURCES CITED

- CyberArk. 2021. Least Privilege. [online] Available at: <<https://www.cyberark.com/what-is/least-privilege/>>.
- CYDEF. 2021. The Human Factor: The Hidden Problem of Cybersecurity - CYDEF. [online] Available at: <<https://cydef.ca/the-human-factor-the-hidden-problem-of-cybersecurity/>>.
- Garska, K., 2018. Healthcare Cybersecurity and the Human Factor: Using Risk-Based Authentication that Considers Behavioral Factors. [Blog] Identity Automation, Available at: <<https://blog.identityautomation.com/healthcare-cybersecurity-and-the-human-factor>>.
- Improving Usability, Safety and Patient Outcomes with Health Information Technology, 2019. Improving Access to Healthcare with Online Medical Appointment System.
- Journal of Medical Internet Research, 2017. Web-Based Medical Appointment Systems: A Systematic Review. [online] Available at: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5425771/>> [Accessed 20 September 2021].
- Solutionreach, 2017. 6 Ways to Schedule Patients Effectively and Efficiently. Available at: <<https://www.solutionreach.com/blog/how-to-schedule-patients-effectively>>.
- Thibodeau, Y., 2018. How Artificial Intelligence Can Impact Medical Scheduling. [Blog] Petal, Available at: <<http://blog.petal-health.com/artificial-intelligence-impact-medical-scheduling>>.
- Zhao, P., Yoo, I., Lavoie, J., Lavoie, B. and Simoes, E., 2017. Web-Based Medical Appointment Systems: A Systematic Review. Journal of Medical Internet Research, 19(4), p.e134.