Assignment 2: Information System Review and Evaluation in the Healthcare Industry

Chenling Zhang 14234049

Department of Information Technology University of Technology Sydney

32557 Enabling Enterprise Information Systems

August 31, 2022

Table of Contents

Task 1

Task 1A

Healthcare Industry: Overview and rationale for choosing it

The healthcare industry in Australia is one of the biggest employers of the economy having more than 1.8 million people to serve patients. It consists of private organisations and Medicare which comes under the universal healthcare system of Australia. The main participants of the industry are hospitals, health providers, medical facilities, and patients (Australian Industry and Skills Committee, 2021). The rationale behind choosing the healthcare industry for analysis is that it is one of the biggest industries that contribute to the growth of the Australian economy and supports the well-being of the people of the country. Hence, it will be interesting to analyse the significance of information technology within the industry.

Digital transformations in the Healthcare industry

With the emergence of information technology, there have been several digital transformations that have occurred within the Australian healthcare industry. Among the many, the two most noticeable digital transformations that happened within the industry are:

I.   Use of big data for predictive analysis

Big Data helps hospitals in the Australian healthcare sector to collect information about the business as well as the patients, their medical history, and transaction history. Using this information hospital administration makes a predictive analysis of the rate of future admission and allocates staff according to that (Karim, Gide, & Sandu, 2019). Similarly, big data is very useful to facilitate preventive healthcare for patients in the future by identifying patients' health conditions from his/her medical history. It has been also found that big data has significantly reduced the cost of the Australian healthcare system.

II.   Use of the Internet of Medical Things for self-care

In recent days, there are several wearables and medical devices that are built upon the Internet of Things that allows patients to track their health conditions and manage diseases by themselves. These devices also come under the Australian Digital Health strategy to educate patients about the technologies that will make them less dependent on the physical presence of

a doctor (Oshni Alvandi, Bain & Burstein, 2021). As such, they can do their self-care and keep a track of their disease.

Task 1B

Implementation of digital transformations as a strategic necessity

The digital transformations made in the Australian healthcare industry have been a part of the strategic necessity. Previously, Australian healthcare systems were facing a huge challenge of medication errors due to the unavailability of patient records. Weingart et al. (2000) identified that a decade ago, the medical error rate in hospitals of NSW was more than 16.6%, which led to a 13.7% disability rate and cause a 4.9% date rate. However, 51% of the error cases were said to be preventable. To resolve this issue, the Australian healthcare system approached big data for gathering information such that they can keep a good track of the medical records of the patients and thus reduce the medical error rate.

In Australia, traditional health literacy and limited digital literacy acted as a barrier to the digital engagement of patients in practising self-care and preventing diseases from getting worsen. The Australian healthcare system finds it essential to develop a Digital Healthcare strategy that incorporates IoT technology to enable the public to take care of their health before it gets worst. Wang, Wu, and Qi (2021) found that with the medical wearables that use the Internet of Medical Things, people can enhance their quality of life, track their physical activities, and gain more knowledge about their health and diseases.

Task 2

Task 2A

Business processes carried out in the healthcare industry

As the Australian healthcare industry comprises several participants like medical service providers, health workers, nurses, and medical specialists, the business process is more single-functional than cross-functional. The healthcare process is divided into two most important processes, namely the medical treatment process and the generic administration process. The medical treatment process is associated with the patient and is operated according to comprising observation, diagnostic-therapeutic cycle, reasoning and action. Under the medical treatment process, the health practitioners like doctors and nurses play an integral role as their
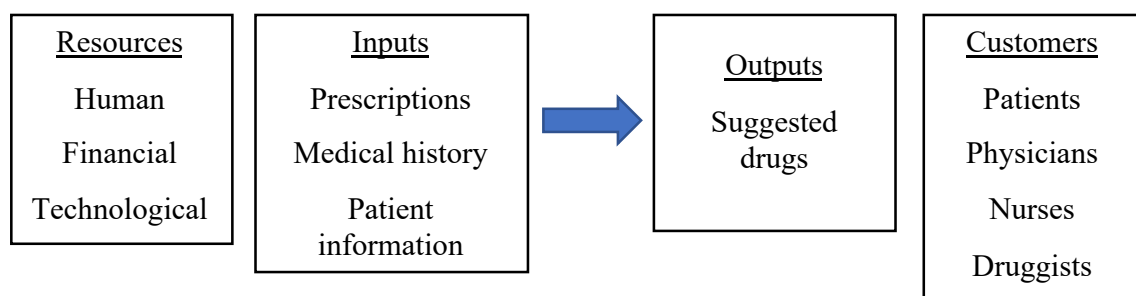
medical knowledge is vital to deal with the specific patient case and interpret the proper medication based on patient-specific information. On the other hand, the administrative process helps the medical treatment process for scheduling patients and processing requests for a health examination. This process does not have to deal with any tailored action but rather coordinates with the medical treatment process to support further treatment (Rebuge, & Ferreira, 2012). The industry has segregated its different business processes into a single-functional team to avoid the delay in processing any information and fulfilling the fundamental needs of the patients without wasting any resources or time. The different processes are continuously measured to assess their efficiency and effectiveness.

Task 2B

Evaluation of a business process

The medical treatment process is associated with a diverse range of inputs, outputs, customers, and resources. The inputs in the process are the prescriptions and drugs that are processed by physicians, nurses and pharmacists to medicate the disease. The input process also involves the application of information systems and technologies like big data to get information about a patient's medical history, a previous visit to the hospital and other essential information that is required before writing a new prescription (Yousef & Yousef, 2017). The outputs of the medical treatment process are the selected drugs that are best suited for the patient. The customers are the physicians, nurses, and patients who purchase the drugs selected for medication. Lastly, the process involves resources like human resources (doctors, nurses, staff), financial resources (finance for purchasing equipment for basic medical inspection), and technological resources (IoT, Big Data).

Figure 1: Flow diagram of the Medical Treatment Process

Resources	Inputs		Outputs	Customers
Human	Prescriptions		Suggested drugs	Patients
Financial	Medical history	→		Physicians
Technological	Patient information			Nurses
				Druggists

Task 3

Discussion of the ethicality, legality, and privacy of the business processes, data collection, data accuracy, and/or data confidentiality as it applies to information systems

Nowadays, the information system has helped the healthcare industry to optimise its business process to a large extent. As the healthcare industry comprises multiple functional business processes, each process aims to perform various takes through a wide spectrum of computer programs (Rainer & Prince, 2021). As healthcare institutions are continuously making effort to utilise the new technologies to acquire a large volume of customer data, they are raising the ethical concern of sharing patient data with third-party entities that might exploit it for commercial profit. The patient's data might also be illegally used for targeting vulnerable populations. In order to maintain the ethicality, legality and privacy of business processes, the Australian Medical Association (AMA) has developed a Code of Ethics, which incorporates the values that need to be abiding by anyone who is associated with the medical profession (AMA, 2017). Under the Code of Ethics, while collecting medical data from patients, healthcare authorities in Australia are required to submit statistical information and data to the Ministry of Health.

From the Health depart of the NSW Government (2015), it has been identified that the data collected must be authorised by some of the healthcare legislation like the Public Health Act 2010, Private Facilities Act 2007 and Community Care Act 1985. To maintain the legality of the data, hospital staff are required to define the purpose of collecting data from the patient or their family members. Healthcare service providers also need to assure patients to keep the confidentiality of the data collected and not release or use patients' personal information without their authorisation. In the healthcare industry, the importance of accurate data is indispensable as it is essential for planning treatment and making vital decisions which might impact the lives of patients. To maintain the accuracy and completeness of medical data, hospital staff or medical practitioners are asked to record information online at the time of medical procedure or consultation so that entries are made according to the correct health condition of the patients. Also, clinicians are directed to make proper and transparent communications with the patient's family relating to the treatment and care of a patient. Such information must be documented in the health record of the patient.

Task 4

Unintentional and/or deliberate threats to information systems in healthcare industry

Table 1: Deliberate and unintentional threats to information systems in the healthcare industry

Potential threats	Description	Nature
Power failure	Server down due to power loss	Unintentional
Network infrastructure failure	Internet connection failure, switch port problem, network software error, unsecured wireless network	Unintentional
Hardware and software failures	Insufficient storage, hardware or software maintenance problem	Unintentional
Operational issues	Lack of IT training for hospital staff	Intentional
Cyberterrorism	Malicious code embedded through usage of mobile and wireless technologies	Intentional
Acts of human failure	Entry of inaccurate data by staff, accidental modification or deletion of data, confidential information transferred to wrong recipient	Unintentional
Social engineering attacks	Accessing confidential information via social media	Unintentional
Environmental support failure	Fire at the server, lightning attacks	Unintentional

(Source: Narayana Samy, Ahmad, & Ismail, 2010)

Discussion on the two of the identified threats

Among the different threats identified above, the two most serious threats to Information Systems are:

    I.   Social Reengineering:

In the healthcare sector, social engineering refers to the practice of manipulation of staff members for giving access to the official routers, computers, or Wi-Fi networks to access the confidential information of patients like protected health information, personal data of patients (debit or credit card number/pin), and install malware that will create a serious challenge in handling the systems in future (Health Sector Cybersecurity Coordination Center, 2022). The different types of social engineering attacks include phishing, smishing, whaling, tailgating, and vishing. Phishing is the most common type of social engineering attack in the healthcare industry as it is done by outsiders to private health service providers to gain patients' personal information from them and later use them in illegal activities. To prevent social engineering, many Australian healthcare centres are updating vulnerable systems, securing backups and authorising multifactor authentication so that any outsider trying to hack the system can be caught instantly (Fraudwatch, 2022). The healthcare sector also gives advanced education around social reengineering to their staff to reduce the risk of getting future attacks.

    II.   Cyberterrorism:

Cyberterrorism or cyberattacks are the most common fraudulent attacks on the Australian healthcare sector in recent days. The cyber-terrorist tries to use malware to compromise the integrity of healthcare institutions' computers or wireless networks and collect information about patient's credit cards and personal health records and modify them so that they can disrupt the health facility needed for patient care (De Cauwer & Somville, 2021). If the hospital lost the patient's data due to the invasion of ransomware, it might put the patient's life at risk. To mitigate the issue, Australian health leaders are spending huge capital on improving cybersecurity by installing features in their systems like password rules, implementation of VPNs, and security updates. But reports suggest that they are still lagging to prevent cyberattacks as cybercriminals are increasing sophistication and expanding their operations to make the attacks stronger (PWC Australia, 2022). Hence, the threat of cyberterrorism is still hovering over the Australian healthcare industry.

Task 5

Self-reflection of learnings

In the current report, I have analysed the different applications of information systems in the healthcare industry. Before doing this project, I had little idea about the importance of information systems in the healthcare industry of Australia. By doing secondary research from the authentic database, I get to know about the strategic need for implementing information systems in the healthcare industry. I used my analysing skill to evaluate the importance of ethicality, legality and privacy in data collection for healthcare services. Also, I got to know how much cyberterrorism and social reengineering are threatening the industry.

Interestingly, from this project, I learned about brainstorming. I learned how to ideas into the discussion in an organised manner without wasting any time. Additionally, I developed the skill of drafting, editing and proofreading, which I lacked before doing this assignment.

References

AMA. (2017). *New Code of Ethics for doctors.* https://www.ama.com.au/media/new-code-ethics-doctors#:~:text=%E2%80%9CThe%20AMA's%20Code%20of%20Ethics,patients%2C%20colleagues%2C%20and%20society.

Australian Industry and Skills Committee. (2021). *Industries / Health.* https://nationalindustryinsights.aisc.net.au/industries/health#:~:text=The%20Health%20Care%20and%20Social%20Assistance%20industry%20is%20the%20largest,than%202.0%20million%20by%202025.

De Cauwer, H. G., & Somville, F. (2021). Health care organizations: soft target during COVID-19 pandemic. *Prehospital and disaster medicine*, *36*(3), 344-347. https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine/article/health-care-organizations-soft-target-during-covid19-pandemic/FA063BA6545BF74084DA10C982D476C6#

Duckett, C. (2018, Octber 29). Phishing spikes as private health continues to be most breached sector in Australia. *ZD Net.* https://www.zdnet.com/article/phishing-spikes-as-private-health-continues-to-be-most-breached-sector-in-australia/

Fraudwatch. (2022). *The modern Australian healthcare: Threats and Solutions.* https://fraudwatch.com/the-modern-australian-healthcare-threats-and-solutions/

Health Sector Cybersecurity Coordination Center. (2022). *The Impact of Social Engineering on Healthcare.* https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf

Karim, S., Gide, E., & Sandu, R. (2019, June). The Impact of Big Data on Health Care Services in Australia: Using Big Data Analytics to Categorise and Deal with Patients. In *Proceedings of the 2019 International Conference on Mathematics, Science and Technology Teaching and Learning* (pp. 34-38). https://doi.org/10.1145/3348400.3348414

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health informatics journal*, *16*(3), 201-209. https://doi.org/10.1177%2F1460458210377468

NSW Government (2015). *PRIVACY MANUAL FOR HEALTH INFORMATION*. https://www.health.nsw.gov.au/policies/manuals/Documents/privacy-manual-for-health-information.pdf

Oshni Alvandi, A., Bain, C., & Burstein, F. (2021). Understanding digital health ecosystem from Australian citizens' perspective: A scoping review. *PloS one*, *16*(11), e0260058. https://doi.org/10.1371/journal.pone.0260058

PWC Australia. (2022). *Proven precautions to help protect health organisations and patients from cyberattacks*. https://www.pwc.com.au/health/health-matters/cyber-security-the-healthcare-sector.html

Rainer, R. K., & Prince, B. (2021). *Introduction to Information Systems. Australia and New Zealand Edition* (8th Edition). Wiley. https://www.wiley.com/en-au/Introduction+to+Information+Systems%2C+8th+Edition-p-9781119594635

Rebuge, Á., & Ferreira, D. R. (2012). Business process analysis in healthcare environments: A methodology based on process mining. *Information systems*, *37*(2), 99-116. https://doi.org/10.1016/j.is.2011.01.003

Wang, C., Wu, X., & Qi, H. (2021, December). A comprehensive analysis of E-health literacy research focuses and trends. In *Healthcare* (Vol. 10, No. 1, p. 66). MDPI. https://doi.org/10.3390/healthcare10010066

Weingart, N. S., Wilson, R. M., Gibberd, R. W., & Harrison, B. (2000). Epidemiology of medical error. *Bmj*, *320*(7237), 774-777. https://doi.org/10.1136/bmj.320.7237.774

Yousef, N., & Yousef, F. (2017). Using total quality management approach to improve patient safety by preventing medication error incidences. *BMC health services research*, *17*(1), 1-16. https://bmchealthservres.biomedcentral.com/articles/10.1186/s12913-017-2531-6