Cibersecurity as a primary technological concern in Telepharmacy

In this digital century, we are heavily relying on Information Technology (IT). However, this IT comes with many vulnerabilities, that is why Hackers represent a well-known threat and are responsible for a significant degree of disruption and damage to information systems[10]. To combat with them, cybersecurity was born.

Cybersecurity is composed of cyber and security. Cyber' as a prefix is forming words relating to the computers, information technology, and virtual reality. Security is defined as the state of being free from danger or threat. Hence, cibersecurity is a field for protection of computer related technologies. The cybersecurity is being required continuously by politicians, computer specialists, IT managers, tech entrepreneurs, health industry professionals and national security operator[1]. If cybersecurity is a kind of that wide, why should we discuss it in Pharmacy (another big prestigious and lovely profession)? It is because of telepharmacy. Telepharmacy is a rapidly growing area of communication which is devised to provide pharmacy operations and patient care at a distance and to expand access to healthcare, enhance patients' safety and improve patient outcomes[2,3]. In this presentation, we used various resources from pubmed, google scholars and newspapers to know why cybersecurity must act as as a primary technological concern in Telepharmacy.

Cybersecurity and telepharmacy are separate fields which are attracting more attention than ever, not just in headlines, but among policymakers, industry leaders, academics, and the public. Cyberattacks are becoming more successful because on internet, no one and nothing is safe[8]. For pharmacies, any compromises to manufacturing, monitoring and delivery systems can result in a loss of integrity and harm to the public. This can cause safety problems, forgery and reputation damage. There is same risks to other medical systmes. Vulnerabilities in the design or implementation of a medical devices such as an insulin pump or in anything interconnected to such devices can result in loss of device integrity and potential harm to patients if they are exploited in a cyberattack[4]. For example, in 2024, UnitedHealth blames a 'nation-state' for a hack disrupting pharmacy order where a hacking attack against a division of UnitedHealth Group has left some pharmacies unable to dispense prescriptions[5]. Not only that but also during 2021 in USA, Hospital, Pharmacy, and Dental Practice Report Hacking Incidents Impact More Than 355,000 Patients[6]**.** Hacking cases in Rwanda are also common, for example Central Bank Governor John Rwangombwa said the bank registered 80 hacking cases as of first season of 2017. In 2016, Police says that Rwanda managed to intercept attempts to steal Rwf1billion and €340 while in 2017 the cyber thieves attempted to walk away with Rwf2billion and $ 605,028 in vain[7]**.**

Cyber security is a critical element of telepharmacy security services, essential for protecting sensitive patient data and ensuring the integrity of telepharmacy operations. Pharmacies handle vast amounts of personal health information, making them prime targets for cyberattacks. To mitigate these risks, pharmacies must implement comprehensive cybersecurity measures, including advanced encryption techniques, firewalls, and intrusion detection systems to protect electronic health records (EHRs) from unauthorized access. Secure access controls, such as

multi-factor authentication and regular password updates, ensure that only authorized personnel can access sensitive information. Regular cybersecurity training for staff is essential to raise awareness about phishing scams, malware, and other cyber threats. Conducting routine security audits and vulnerability assessments helps identify and address potential weaknesses in the system. Additionally, maintaining up-to-date software and systems is crucial to avoid latest cyber-attacks. By prioritizing cybersecurity, telepharmacy operators can safeguard patient data, ensure compliance with regulations, and maintain the trust and confidence of their patients, ultimately supporting a secure and reliable pharmacy environment[9].

Conclusively, even if telepharmacy is going to play key roles in our population's health, it is vulnerable to security threats due to interconnected, easily accessible access points, outdated systems, software tools and a lack of emphasis upon cybersecurity. We must focus on patient care. However, healthcare technologies hold vast amounts of valuable, sensitive data. In many cyberthreats financial gain is the motivation for attacks because medical identity is more valuable than any other identity credentials[11]. So as Pharmacists, we must work hard to protect ourselves and the public.

References:

1. Bay M. What is cybersecurity. French Journal for Media Research. 2016;6:1-28.
2. Omboni S, Tenti M. Telepharmacy for the management of cardiovascular patients in the community. Trends Cardiovasc Med. 2019 Feb;29(2):109-117. doi: 10.1016/j.tcm.2018.07.002. Epub 2018 Jul 12. PMID: 30037524.
3. Le T, Toscani M, Colaizzi J. Telepharmacy: A New Paradigm for Our Profession. Journal of Pharmacy Practice. 2018;33(2):176-182. doi:10.1177/0897190018791060
4. Jaithliya T. Cyber security in pharmacy and pharmaceutical companies. J Pharm Sci. 2017;2.
5. Pashankar, J. R. J. T. a. S. (2024, February 23). UnitedHealth blames 'nation-state' in hack disrupting pharmacy orders - Los Angeles Times. *Los Angeles Times*. https://www.latimes.com/business/story/2024-02-23/unitedhealth-blames-nation-state threat-in-hack-disrupting-pharmacy-orders?
6. Hospital, Pharmacy, and Dental Practice Report Hacking Incidents Impact More Than 355,000 Patients. Steve Alder Year: 2021 Container: The HIPAA Journal. https://www.hipaajournal.com/hospital-pharmacy-and-dental-practice-report-hacking-incidents-impacting-more-than-355000-patients/?
7. Sabiiti, D. (2018, January 19). How Rwanda stopped eight million cyber attackers. *KT PRESS*. https://www.ktpress.rw/2018/01/how-rwanda-stopped-eight-million-cyber-attackers/
8. Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, Christopher Millard, The rise of cybersecurity and its impact on data protection, *International Data Privacy Law*, Volume 7, Issue 2, May 2017, Pages 73–75, https://doi.org/10.1093/idpl/ipx009
9. Anjali P. Pharmacy Safety Essentials and Protecting Patients and Ensuring Security.
10. Furnell SM, Warren MJ. Computer hacking and cyber terrorism: The real threats in the new millennium? Computers & Security. 1999 Jan 1;18(1):28-34.

11. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul 1;113:48-52.