Summary Post

Data accessed illegally can be used as ransom, to commit tax frauds, to provide supporting disability documentation, to send fake bills to insurance providers, to obtain healthcare, prescription drugs, medical treatment, and to obtain government benefits like Medicare and Medicaid.

The evolution of  Internet of Things, (IoT) comes with significant challenges  such as hijacking of IoT devices, financial crime, home invasion etc as seen in the article on mannequins, therefore, it is important cyber security measures are put in place wherever there is sensitive data.(Kumar, 2017)

 I like the point raised by David on the  NHS Digital (2020) recommendations  for fewer routes to unpatched software. A lot of smart devices were developed without security in mind probably due to limited resources, therefore, these devices don’t  support the processing power needed for secure communication like encryption and  are not designed to accommodate software or firmware which makes vulnerability patching difficult. In addition to software patching and encryption etc Security by Design (SBD) will  ensure devices connected to the internet are secure.(*Cybersecurity in the Internet of Things: Legal aspects | Elsevier Enhanced Reader*, no date)

REFERENCES

*Cybersecurity in the Internet of Things: Legal aspects | Elsevier Enhanced Reader* (Accessed 22 May 2021). doi: 10.1016/j.clsr.2016.07.002.

Kumar, C. J. (2017) ‘New Dangers in the New World: Cyber Attacks in the Healthcare Industry’, 10(3), p. 15.

Cybersecurity in the Internet of Things: Legal Aspects | Elsevier Enhanced Reader’.. [**https://doi.org/10.1016/j.clsr.2016.07.002**](https://doi.org/10.1016/j.clsr.2016.07.002)