 doi:10.20944/preprints202001.0359.v1

INTERNET OF THINGS IN HEALTHCARE:

The Social, Ethical, Legal & Professional Implications.

Otobong Inieke

Independent Researcher, Department of Computing – Graduate of Middlesex University, Mauritius Campus.

otobonginieke@gmail.com

https://orcid.org/0000-0001-9906-4028

https://devinieke.com.ng

Abstract: Implications of the novel usage adoption of the internet of things in various sectors of works and life are researched and documented at pace. This is related to the overall high rate at which new technologies are adopted in modern society. Healthcare is a vital aspect of everyday activities and as such overlaps with the increasingly important role played by use of the internet and associated technologies. The purpose of this review article is to draw attention to the potential social, ethical, legal and professional limitations to using IoT in the context of healthcare. The social and ethical aspects in particular, focus on IoT usage in care of the elderly with relevant case studies as reference.

Keywords: Internet of things, healthcare, ethics, data privacy.

Type: Review.

Introduction

In a world with constant advancement in technology, there is the ever present need for improved transmission of information and better convenience in our interaction with connected devices. As a concept, the internet of things generally refers to the connection, interaction and sharing of contextualised data between sensors, devices and systems using the internet with the aim of increasing efficiency in a given situation (Burgess, 2018). The internet of things, though in its nascent stages already permeates most of today's society and can be observed in use-cases ranging from home automation systems and fitness trackers to energy management and healthcare (FTC Staff, 2015). According to (Meola, 2018), by 2020, there will have been approximately a $6billion investment into the aspects of IoT such as development, connectivity, integration, security and storage. As far as the benefits and potential pitfalls of this emerging technology are concerned, the major stakeholders in this regard are; the consumers, governments and businesses (Meola, 2018).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2020 doi:10.20944/preprints202001.0359.v1

Though the positive impact of the Internet of Things is profound, there are numerous negative implications to be considered. There is the implicit knowledge that for the devices making up an IoT ecosystem, massive amounts of data will be mined for optimal communication between these devices. This brings up questions surrounding consumer privacy and security of harvested data (parliament.uk, 2015). The current debates about IoT basically address issues such as; anonymity when using IoT devices and services, the potential of turning a regular IoT device into a security or privacy target, consumer awareness of the special capabilities of these IoT devices and the control of the flow of data between these systems (mhc.ie, 2014).

IoT in healthcare currently incorporates other technologies such as machine learning and big data. Physicians and related professionals are now, more than ever able to get detailed insights allowing for precise levels of action to be taken at the point of care (Lee, 2015).

IOT in the Healthcare Industry – Uses & Limitations

Technology based on the internet of things has woven its way into everyday consumer devices and one aspect of our lives that has also been impacted is healthcare. In recent times, people have been able to schedule medical appointments and receive tentative advice through applications on smartphones and devices without calling a hospital, making a trip to the clinic or waiting a long time for a scheduled meeting (Neelam, 2017). By taking advantage of connected devices and sensors such as weight scales and blood pressure monitors, patient information could be viewed and real-time diagnostics could be provided which is potentially life-saving (ibid. p11). Aside from bed-side monitoring and preventive care, IoT also serves the healthcare industry through personal care solutions. People use wearable sensors connected to applications running on personal devices to track activities such as calories burned during exercise or number of steps taken during a certain period while the applications suggest possible lifestyle changes to prevent health issues (Miorandi, Sicari, Pellegrini, & Chlamtac, 2012).

Pacemakers and wireless insulin pumps are examples of IoT devices that can pose critical risks if they are compromised in any way. In this situations, threats to the functionality of such devices take precedence over breach of data (Choufanni, 2014). In 2011, during a Black Hat conference, a cyber threat analyst demonstrated the vulnerabilities of healthcare IoT systems. The analyst who is diabetic, exploited security gaps in his own insulin pump causing it to respond to a remote control device and also altered the reading on his glucose monitor by intercepting its wireless signals (Steciw, 2011). Further reports showed that although the device manufacturers were alerted to the issues uncovered, insufficient action was taken which prompted two members of the American congress to request a review of the Federal Communication Commission's policies regarding wireless devices (Steciw, 2011).

Admittedly, medical IoT devices can be accessed to have their software and firmware updated with latest anti-malware protections thus preventing or reducing the chances of such incidents. This is not the case if such devices are implanted, such as pacemakers and artificial pancreases,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2020 doi:10.20944/preprints202001.0359.v1

this is a serious limitation to the adoption of IoT in certain aspects of healthcare due to the fact that vulnerabilities in IT are almost always addressed retroactively (Choufanni, 2014).

The lack of fully deployed IoT systems is a key indicator that the technology is still in its early stages. Examples of problems with the technology itself include the long term effects of electromagnetic radiation on people and signal strength issues within hospitals (Laplante & Laplante, 2016). Due to the fact that sensors and devices within the IoT ecosystem are always connected, it goes without saying that security is of utmost importance to the increased adoption of the technology within the healthcare industry (Miorandi, Sicari, Pellegrini, & Chlamtac, 2012). The stakeholders in this context will remain unwilling to adopt IoT in this domain if there are no guarantees in privacy, trust and authenticity (ibid .p1505).

With the aforementioned guarantees in IoT security, standard requirement for a healthcare system would in the least include the following; Resistance to malicious attacks in the sense that single points of failure within the system are to be avoided and the system should also adjust itself to counter tangential failures; Authentication of data which means that all object addresses and information transmitted within the system should be authenticated; Control of access whereby administrators and information providers can setup a level of access control for data provided and finally privacy measures that only the information provider can deduce when using an observation interface within the system (Tarouco, et al., 2012). It has been observed that malicious attackers who focus on mobile devices usually have defined goals such as taking patient or user information, damaging system resources and even shutting down critical applications. The many threats around mobile devices in healthcare IoT are basically derived from regular computing systems which leaves them vulnerable to attacks like Distributed Denial of Service (DDOS) and Routing Diversion Attacks (Tarouco, et al., 2012).

Although IoT in healthcare is still a new concept to many professionals in the industry, its implementation is inevitable. The advantages are being realised but adaptable systems are yet to be deployed and the significant obstacles have not been overcome (Laplante & Laplante, 2016).

Ethical Issues

Although the benefits of IoT in healthcare are numerous, it raises ethical issues based on the vulnerabilities of devices that connect to the internet, the sensitive nature of health related data and the impact on healthcare delivery (Mittelstadt, 2017). The Internet of things in healthcare is built to operate within public and private domains. The sensors and devices are carried around by an individual or situated within environments like hospital wards, a home or a workplace. These situations create the opportunity for data about an individual’s behaviour or health status to be collected and analysed by a third party (Mittelstadt, 2017). Although healthcare is being improved through remote monitoring and quicker response times, the nature of the technologies involved simultaneously create opportunities for breaching personal or data privacy.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2020 doi:10.20944/preprints202001.0359.v1

Certain IoT applications are both ethical and unethical depending on the concerned stakeholder, IoT devices and sensors tend to be forgotten about if they are unobtrusive or discreetly embedded in an environment. The validity of the user's consent to be closely observed is eroded if they forget they are being monitored (Gaskell, 2017). Considering the consequentialist theory of ethics, which posits that '*the morally right action is the one with the best overall consequences* (Haines, n.d.)*'*, the application of IoT in this context is ethical because the user gave consent to be monitored and the recorded data is analysed for their own well-being. On the other hand, an individual's sense of autonomy and privacy is disrupted if they know that they are constantly monitored (Mittelstadt, 2017). For this reason, the application of IoT in this context can be debated as unethical because according to deontology, '*an act is only good if it conforms to moral rights* (Gamlund, 2012)'.

It has also been seen that the way IoT is used in healthcare can impact the delivery of healthcare services. In a bid to protect a sense of autonomy especially in the elderly, they are provided with greater power over their own care through the use of less intrusive IoT devices like bracelets or armbands. This reduces visits from healthcare personnel and can lead to possible isolation since monitoring can be done remotely (Gaskell, 2017). Following Kant's beliefs that "*rationality is the ultimate good*" and "*people are fundamentally rational beings*" (Barlow, 2018), it can be argued that the actions toward preserving the sense of autonomy in elderly people are ethical. Alternatively, the fact that risk of isolation is a major concern of the elderly in this context, the action can be queried as unethical because according to the utilitarian school of ethical thought; '*the moral worth of an action is determined by its contribution to increasing happiness in people*' (Arpaly, 1998).

Feedback from smart applications can cause users to alter their behaviour to be in line with the device's expectation e.g. a smartwatch suggests a calorie drop in diet to lose a certain amount of weight in a specified time according to its own calculations (Mittelstadt). The question here is whether the user's behaviour is altered based on self-interests or to be aligned with the service that the user agreed to i.e. personalised feedback (ibid.p5). Undermining a user's autonomy through product design must be weighed against the perceived benefit meaning the design is unethical if the user is influenced towards third party interests. On the other end, such influence is considered ethical if the altered behaviour leads to better health. Utilitarianism supports the first argument because it is concerned with the outcome of an action which in this case does not favour the concerned individual (Haines, n.d.) While the subsequent argument is backed by Deontology which is focused on rationalism and the fact that deciding to take perceived positive action is good (Alexander & Moore, 2016).

These are but a few ethical challenges that currently plague the rapid adoption of Internet of Things in the healthcare industry.

Social Issues

Emerging technologies such as IoT can be used to the benefit of society, an example of this is the 'Smarter Living' project being run by IBM in the city of Bolzano Italy. This is a city where

 doi:10.20944/preprints202001.0359.v1

1 in 5 people are over the age of 65. The aim of the project is to help the elderly live better and longer in their homes while improving the efficiency of caretakers through the use of technology (IBM.com, 2014). Touchscreens and various interfaces are used to allow the users request assistance, ambient sensors allow smoke, temperature and humidity levels to be monitored while personal sensors provide health based telemetry (IBM.com, 2014). These systems work in tandem to assist the elderly which has the run-off effect of improving their feelings of self-worth while simultaneously relieving pressure on healthcare services (BCS.org, 2014).

Admittedly, the rapid advancements in IoT related technologies have been beneficial to society with adoption in healthcare and educational industries, it must also be noted that the technology also has negative implications (IEEE, 2017). Generally, devices used in healthcare IoT fall between consumer facing devices for measuring fitness or overall wellness and clinical devices meant for patients. In most cases, the consumer based devices are built with attractive designs which intrigues people and is less likely to carry a social stigma such as the Microsoft Band 2 which is a bracelet that tracks calories burned during exercise and sleep patterns (Faulkner, 2016). This is not the same for individuals with medical conditions that require the usage of health IoT devices. The issue for such an individual is dealing with the stigma that is connected with using such devices which may in turn be associated with a health or disease condition (Mittelstadt, 2017).

Following the scenario above, it has been observed that elderly individuals in care homes who require visible applications of healthcare IoT devices like oxygen masks feel more vulnerable as this is an indicator of frailty. The devices in such scenarios, affect a person's ability to control how they are perceived, therefore the power to manage public identity is eroded (Mittelstadt, 2017). Furthermore, the knowledge that one is being monitored has been seen to negatively affect the regular behaviour and sense of autonomy of elderly people. The obtrusive nature of some of the healthcare IoT devices has also been observed to reduce risky behaviours in ageing users and this is considered negative because such behaviours in elderly people can signify the desire to maintain independence which is inherently a human characteristic (Percival & Hanson, 2006).

The societal impact of IoT in healthcare revolves around privacy. The problem comes from the fact that for a user's privacy to be protected, the individual must give consent relating to how information is transmitted between IoT devices and what kind of action is taken by the sensors and systems. Conversely, the design of IoT in any domain is based on the continuous interaction between devices with the aim of autonomous or 'smart' decision making (Ebersold & Glass, 2016). Additionally, there is the chance that an individual feels a loss of control due to the fact that IoT-based data is constantly transferred among other devices and decisions that can have personal effect are made without the awareness of said individual. Such lack of control or unwilling participation can lead to the compromise of a person's sense of freedom (Ebersold & Glass, 2016).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2020 doi:10.20944/preprints202001.0359.v1

Legal Issues

Following the rapid development of IoT, the merge between the application of the technology and the healthcare industry has caused a massive expansion in the scope of medical data. Furthermore, regulations and legal constructs protecting usage of such data have not kept up with the technology (Zhu & Zhan, 2017). The problems debated concern data ownership, appropriate privacy policies, user control and general liability (Cohen, 2016). In 2015, the Federal Trade Commission (FTC) levelled charges of false advertisement against Health Discovery Corporation (HDC), the promoters of an application called MelApp (Clark, 2015). The application supposedly assessed the risk of melanoma using image and pattern recognition algorithms, upon investigation, the FTC found that the claims were false and HDC had violated Section 5a of the Federal Trade Commission Act which states that '*unfair or deceptive acts or practices in or affecting commerce are declared unlawful*' (ftc.gov, 2008).

In relation to data ownership and access, provisions within the recently enforced General Data Protection Regulation (GDPR) strengthens an individual's right to not only confirm what information an organisation has on them but access that information as well as any other related information (Burgess, 2018). The North-eastern University located in Boston, United States, conducted an experiment involving over 17,000 Android applications, the experiment showed that over 9,000 of the applications had access to a smartphone's camera and microphone while over 8,000 sent screen recordings and app interactions to Facebook and a third party called AppSee which is a mobile analytics company (Hill, 2018). The above case is an illustration that shows how easy a third party can gain control of private and potentially impactful information without the express consent of an individual. According to Article 22.1 of the GDPR, an individual has the right to not be subject to a decision based solely on automated processing including profiling. Furthermore, a caveat is included in Article 22.2c which states that Article 22.1 does not apply if explicit consent is not given (Intersoft Consulting, 2018). The result of the university's study shows proof that the actions of the application developers as well as third parties are legally questionable due to the fact that user of the application may have given usage consent to the developers but not for the transfer of data to unknown third parties (Hill, 2018).

As mentioned previously, liability is a source of concern in the application of IoT, the following are some of the questions that need to be reviewed; who is responsible for updating software to make sure that IoT devices remain secure, what is the patient's fate if the medical provider goes out of business and who is held responsible if the internet connection is lost during medical application (AboBakhr & Azer, 2017). In a bid to guard against some of this, Article 20.1 of the GDPR states in part that an individual has the right to request personal data in a '*structured, commonly used, machine-readable format*' to be transferred to another service provider without obstruction (Intersoft Consulting, 2018). Additionally, Section 56.1 of the Data Protection Act 2018 (DPA) summarily states that a data controller must apply all appropriate measures to ensure safety and integrity of an individual's data (legislation.gov.uk, 2018).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2020 doi:10.20944/preprints202001.0359.v1

Professional Issues

Under the auspices of the GDPR and the DPA 2018, healthcare professionals as well as the manufacturers of IoT devices used in healthcare have been saddled with the responsibility of ensuring the integrity of user generated information (Twentyman, 2017). Industry professionals face solution problems when many devices come through hospitals from various sources, this makes adoption difficult because the devices rarely have similar operating systems, encryption protocols or hardware versions (Lee, 2015). A research carried out by SpiceWorks which is an IT community surveyed about 440 IT professionals and showed that security investment was not a top priority even though 86% of respondents expected IoT to raise privacy and security issues (Flinders, 2014). In comment to the study, the IT program manager at SpiceWorks Kathryn Pribish pointed out that though the industry professionals generally accept the inevitability of IoT, those who do not prepare sufficiently will be left behind (Flinders, 2014).

Additionally, IT professionals are urged to maintain relevant knowledge of appropriate laws and regulations when executing responsibilities, this is seen in Section 2.d of the BCS code of conduct which says that one should know, understand and comply with legislation when carrying out professional duties (The British Computer Society, 2015). However, professionals and application developers must make certain that users of their products when giving consent are completely aware of the extent to which their information will be used (Hill, 2018).

An article published by the Wall Street Journal showed that Return Path Inc., a data marketing company had employees who read approximately 8,000 emails in order to 'train' the company's software. Within the same article, Thede Loder the former Chief Technology Officer of a rival company DataSource Inc., said it has become common practice to let employees read user emails in such companies (MacMillan, 2018). Further reporting showed that both companies detailed the practice within user agreements and had strict regulations concerning read emails, this ultimately lead to a loss in customer trust regardless of the constant promise of data protection by related internet companies like Facebook and Google (LeFebvre, 2018). Such a situation is an example whereby insufficient communication between IT professionals and consumers produces unsavoury results. Though the company may have adhered to Section 1.b of the BCS Code of Conduct which states that one must have due regards for the rights of a 3rd party (The British Computer Society, 2015), its actions could still be viewed as unprofessional from the perspective of external stakeholders (the users) because Section 4.a - which says that personal duty must be upheld and disreputable actions must be avoided (The British Computer Society, 2015) - was disregarded.

Conclusion

The internet of things is a boon to society, the rapid development and integration into different parts of our lives has brought improvements. Healthcare is yet to see a full-fledged implementation of the technology because of the fast moving nature of IoT advancement. The reality is that society is still trying to grasp the implications of the technology and more importantly how well it can be leveraged in the safe care of ailing and elderly individuals. The

 doi:10.20944/preprints202001.0359.v1

course of this article has covered the advantages of IoT in healthcare as well as the socio-ethical implications of its application. Data privacy, legal concerns and aspects relating to responsibility were also addressed and it has been made obvious that as far as the full potential of IoT applications in healthcare is concerned, society is yet to scratch the surface.

Acknowledgement

This is to thank all those who provided support in the research, synthesis and completion of this review article. Ilrshaad Goolamally, my project tutor whose crucial guidance helped with the initial research focus and structure. Finally, my unending gratitude goes to my elder sister, Enoh Inieke, for sponsoring my education, without which none of this would be possible.

References

AboBakhr, A., & Azer, M. A. (2017). *IoT Ethics Challenges and Legal Issues.* Cairo: Nile University.

Alexander, L., & Moore, M. (2016). *Deontological Ethics* (Winter 2016 ed.). California: Metaphysics Research Lab, Stanford University. Retrieved July 8, 2017, from https://www.philosophybasics.com/branch_deontology.html

Arpaly, N. (1998). *In Defense of Deep Virtue Ethics.* California: Stanford University. Retrieved from https://www.philosophybasics.com/movements_utilitarianism.html

Barlow, J. M. (2018). *Gale Researcher Guide for: Immanuel Kant.* Michigan: Gale, Cengage Learning. Retrieved from https://www.philosophybasics.com/movements_kantianism.html

BCS.org. (2014). *IoT: Health, ethics, benefits, fears... and more*. Retrieved July 8, 2018, from https://www.bcs.org/content/ConWebDoc/53647

Burgess, M. (2018). *What is GDPR? The summary guide to GDPR compliance in the UK*. Retrieved July 10, 2018, from http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Burgess, M. (2018). *What is the Internet of Things? Wired Explains*. Retrieved May 22, 2018, from http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

Choufanni, R. (2014). *Hospital IT departments fight to keep healthcare BYOD safe*. Retrieved July 20, 2018, from https://searchhealthit.techtarget.com/tip/Hospital-IT-departments-fight-to-keep-healthcare-BYOD-safe

Clark, D. S. (2015). *FTC in the matter of Health Discovery Corporation*. Retrieved July 10, 2018, from https://www.ftc.gov/system/files/documents/cases/complaint.pdf

Cohen, M. H. (2016). *The Internet of Things (IOT) Legal and Regulatory Issues*. Retrieved July 10, 2018, from https://michaelhcohen.com/2016/01/the-internet-of-things-iot-legal-and-regulatory-issues/

Cuijpers, C., & Koops, B.-J. (2008). *The 'smart meters' bill: a privacy test based on article 8 of the ECHR.* Tilburg: Tilburg University.

Ebersold, K., & Glass, R. (2016). The Internet of Things: A Cause for Ethical Concern. *Issues In Information Systems, 17*(4), 145-151.

Faulkner, C. (2016). *Microsoft Band 2: Curves and sensors in all the right places*. Retrieved July 9, 2018, from https://www.techradar.com/reviews/wearables/microsoft-band-2-1306006/review/4

Flinders, K. (2014). *IT departments unprepared for internet of things*. Retrieved July 10, 2018, from https://www.computerweekly.com/news/2240222183/IT-departments-not-preparing-for-Internet-of-Things-despite-expecting-it

FTC Staff. (2015). *Internet of Things - Privacy & Security in a Connected World.*

ftc.gov. (2008). *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*. Retrieved July 10, 2018, from https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority#N_1_

Gamlund, E. (2012). *Ethics.* Bergen: University of Bergen.

Gaskell, A. (2017). *The Ethics Of IoT Usage In Healthcare*. Retrieved July 7, 2018, from https://www.huffingtonpost.com/entry/the-ethics-of-iot-usage-in-healthcare_us_58da21c1e4b0e6062d9230b6

Haines, W. (n.d.). *Consequentialism*. Retrieved August 6, 2019, from https://www.iep.utm.edu/conseque/

Hill, K. (2018). *These Academics Spent the Last Year Testing Whether Your Phone Is Secretly Listening to You*. Retrieved July 10, 2018, from https://gizmodo.com/these-academics-spent-the-last-year-testing-whether-you-1826961188

IBM.com. (2014). *Smarter Care in Bolzano*. Retrieved July 9, 2018, from https://www.ibm.com/blogs/emerging-technology/projects/smarter-care-in-bolzano/

IEEE. (2017). *Social Implications of IoT Technology*. Retrieved July 9, 2018, from http://transmitter.ieee.org/social-implications-iot-technology/

Intersoft Consulting. (2018). *Art.22 GDPR- Automated Individual Decision-making including Profiling*. Retrieved July 10, 2018, from https://gdpr-info.eu/art-22-gdpr/

Intersoft Consulting. (2018). *Article 20 - Right to Data Portability*. Retrieved July 10, 2018, from https://gdpr-info.eu/art-20-gdpr/

Laplante, P. A., & Laplante, N. (2016). The Internet of Things in Healthcare - Potential Applications and Challenges. (I. Bojanova, Ed.) *IT Pro*, 2-3.

Lee, K. (2015). *Healthcare IoT security issues: Risks and what to do about them*. Retrieved July 10, 2018, from https://internetofthingsagenda.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them

Lee, K. (2015). *What's the potential of pairing data analytics and IoT in healthcare?* Retrieved July 20, 2018, from

https://internetofthingsagenda.techtarget.com/answer/Whats-the-potential-of-pairing-data-analytics-and-IoT-in-healthcare

LeFebvre, R. (2018). *Third-party app developers could be reading your Gmail*. Retrieved July 10, 2018, from https://www.engadget.com/2018/07/03/third-party-app-developers-reading-gmail/

legislation.gov.uk. (2018). *Data Protection Act 2018*. Retrieved July 10, 2018, from http://www.legislation.gov.uk/ukpga/2018/12/section/56/enacted

MacMillan, D. (2018). *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*. Retrieved July 10, 2018, from https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442

Meola, A. (2018). *What is the Internet of Things (IoT)? Meaning Definition*. Retrieved May 22, 2018, from http://www.businessinsider.com/internet-of-things-definition?IR=T

mhc.ie. (2014). *The 'Internet of Things' - 10 Data Protection & Privacy Challenges*. Retrieved May 22, 2018, from https://www.mhc.ie/latest/blog/the-internet-of-things-10-data-protection-and-privacy-challenges

Miorandi, D., Sicari, S., Pellegrini, F. d., & Chlamtac, I. (2012). Internet of Things: Vision, Application & Research Challenges. *Ad Hoc Networks, 10*, 13.

Mittelstadt, B. (2017). *Ethics of the health-related internet of things: a narrative review.* London: Springer.

Mittelstadt, B. (n.d.). Designing the Health-Related Internet of Things:. *Information, 8*(77), 5.

Neelam, S. (2017). *Internet of Things in Healthcare.* Kalskrona: Blekinge Institute of Technology.

parliament.uk. (2015). *The Internet of Things: Key issues for the 2015 Parliament*. Retrieved May 22, 2018, from https://www.parliament.uk/business/publications/research/key-issues-parliament-2015/technology/internet-of-things/

Percival, J., & Hanson, J. (2006). Big brother or brave new world? Telecare and its implications for older people's independence and social inclusion. *Critical Social Policy, 26*(4), 888-909.

Popescul, D., & Georgescu, M. (2013). Internet of Things - Some Ethical Issues. *The USV Annals of Economics and Public Administration , 13*(2), 208.

Steciw, A. (2011). *Insulin pump hack reveals lack of medical device security*. Retrieved July 20, 2018, from https://itknowledgeexchange.techtarget.com/healthitpulse/insulin-pump-hack-reveals-lack-of-medical-device-security/

Tarouco, L. M., Bertholdo, L. M., Granville, L. Z., Arbiza, L. M., Carbone, F., Marotta, M., & Santanna, J. J. (2012). *Internet of Things in Healthcare : Interoperability & Security Issues.* Porto Alegre, Brazil: Institute of Informatics.

The British Computer Society. (2015). *Trustee Board Regulations - Schedule 3 Code of Conduct for BCS Members*. Retrieved July 10, 2018, from https://www.bcs.org/upload/pdf/conduct.pdf

Twentyman, J. (2017). *GDPR could have connected healthcare providers feeling queasy in 2018*. Retrieved July 10, 2018, from https://internetofbusiness.com/gdpr-connected-healthcare-providers-feeling-queasy-2018/

Weaver, K. T. (2014). *Smart Grid Awareness*. Retrieved July 8, 2018, from https://smartgridawareness.org/2014/11/03/smart-meter-privacy-invasions-not-justified/

Zhu, M., & Zhan, R. (2017). *China: Big Data Policy And Legal Issues In The Healthcare Industry* . Retrieved July 10, 2018, from http://www.mondaq.com/china/x/557158/Healthcare/Big+Data+Policy+And+Legal+Issues+In+The+Healthcare+Industry