Always Connected: The Security Challenges of the Healthcare Internet of Things

Patricia A H Williams
Flinders Digital Health Research Ctr, Flinders University
Adelaide, Australia
patricia.williams@flinders.edu.au

Vincent McCauley
Emerging Systems – Telstra Health
Sydney, Australia
Vincent.McCauley@health.telstra.com

***Abstract*— In an environment that is only now addressing the security issues of medical devices as a constituent part of IT networks, a new wave of technological development is threatening to swamp healthcare. The Healthcare Internet of Things (HIoT) encompasses the new embedded sensing capabilities of devices together with the availability of always being connected, to improve patient care whilst reducing costs. This development highlights existing security threats as well as creating new vulnerabilities, making the once comprehensive endpoint data transfer frameworks less identifiable and challenging current techniques for information security. This paper reviews the new environment using HIoT, to identify the challenges for security and the impact of this on interoperability in the healthcare setting. Each device and sensor is a potential point of vulnerability for entire networks. The low power design, limited processing and storage capabilities, together with a lack of standard interfaces will also add to the complexity of effective security solutions. Understanding these challenges is vital for anyone engaged in healthcare, as the impact of HIoT will be far-reaching for patients, clinicians, healthcare providers, and healthcare delivery. Making security the enabler of safe and protected data transfer, exchange, and use, is fundamental to using this technology.**

***Index Terms*—Medical informatics, medical devices, data security, computer security, information science, privacy.**

I. Introduction

The Healthcare Internet of Things (HIoT) is not just another wave of technology and consumer gadgets. The concept of Internet-connected devices, transferring data through the web, the cloud and traditional communication media, has seen the smart phone, mobile apps, and medical devices begin to converge [1]. Many aspects of our lives are already impacted by this technology yet it is challenging industry, communications, health, economics, business models, IT, and security [2]. Potentially, real time patient care will undergo a huge transformation with increased availability and the connectivity between sensors, medical devices, mobile technology, and clinical information systems [3].

The HIoT market is expected to reach $117 billion by 2020 [4], involving some 26 billion devices [5]. This market for essentially 'smart sensors' and personal monitoring devices will allow streaming of data in massive quantities. However, quantity and opportunity does not equate to benefits in healthcare and will not until we can find effective and efficient ways to harness this creation and transfer of data. As with any new technological advance, the time to demonstrate effectiveness and potential cost saving, particularly in the healthcare environment often is not realized until the technology is well established. This is further complicated by the challenges of integration with current clinical and health care processes. HIoT will dramatically affect patient monitoring and personalized treatment outcomes [6]. Thus, the challenge is how to harness the meaning of the data to improve healthcare. This is particularly relevant in developing models to triage information and make this information useful in the practice of medicine and in personal health management. Further, healthcare is a special case where the quality, provenance, traceability, integrity and authenticity of the data is vitally important. It is not sufficient to simply sense and transfer data; to be useful from a clinical perspective the origin of the data must be known and be assured that it has been secure during all transfer activities. Thus, HIoT data protection and security are vital.

There are many barriers to address before we can realistically expect results. These range from the regulatory medical device environment, diversity of devices, trusted networking, organizations boundaries and therefore control, the technical debt of device engineering, patient safety, dynamic connectivity, privacy, and the management of the security function, not to mention change management of the complex human interactions. These barriers may mean the harnessing of the potential benefits of HIoT will be more conservative in healthcare than other industry sectors. However, there is no shortage of potentially useful but offbeat sensing devices such as "smart utensils" that help to monitor eating habits, smart socks to measure pressure in order to improve running performance and a smart diaper which notifies parents when it needs to be changed. [7].

It is not the digital sensing nor the computing and communications architectures that have changed; it is the techniques to use these synergistically. Whilst there exist notable cases of security incidents with IoT, the risk of cyber-attacks in the health environment are less well recognized or effectively understood. High profile incidents include: the Chrysler Jeep car recall in 2015 to correct a vulnerability in the 3G data connectivity feature following the demonstration of a successful hack in which many of the car functions could be

978-1-5090-4130-5/16/$31.00 ©2016 IEEE

controlled, including control of the steering [8]. From a healthcare perspective, research by students at the University of Alabama demonstrated, the theoretical ability to kill a robotic dummy patient with an implanted pacemaker by compromising the Wi-Fi communication, and controlling the device remotely. There have been other similar examples using drug infusion pumps [9]. Many medical devices still use outdated embedded software and operating systems, due in no small part to the cost of re-certifying updated devices [10].

Healthcare is contextual and personal, and advances in HIoT together with big data and precision medicine will alter healthcare to improve quality and efficacy of treatment. The context of an individuals' life and how each person lives it (through personal tracking) will be a rich input source to these advances. With 70% of IOT devices found to have serious security vulnerabilities, including using unencrypted network services, weak password requirements, user interface persistent weak credentialing, and 90% of devices collecting personal information [11], the problem is multifaceted and complex. Healthcare is especially challenging because of the diverse environment of operation and the complex regulatory environment. This paper raises awareness and discusses the particular issues that are especially important in digital health.

II. What is the Internet of Things?

The terminology around the Internet of Things (IoT) has seen the development of various derivatives, particularly in health. The IoT is the connection of physical devices and objects that can connect and communicate through Internet technologies using communication systems and sensors. The range of applications for IoT is immense from the connection of a house lighting system to a smart phone, vehicles connecting automatically to GPS and traffic applications, to personal health data monitoring and sharing with your doctor. IoT in healthcare has been driven by falling sensor cost and improved technology [12] including the development of IPv6 so that billions of devices can have an internet address, together with the changing chronic disease profiles, and the transfer of responsibility back to the patient.

HIoT consists of medical devices (divided into categories of wearable external medical devices, implanted medical devices, and stationary medical devices), systems and software, connectivity technologies, services and applications. These technologies are not new to healthcare, having had data transfer and communication ability for some time. However, the change is the interconnectedness of devices into similar networks.

The Internet of Medical Things (IoMT) has been defined as "the collection of medical devices and applications that connect to healthcare IT systems through online computer networks" [13]. This includes the use of remote monitoring, patient tracking devices and wearables. The Internet of Things for Medical Devices (IoT-MD) is closely related to IoMT and is defined as where "wearable devices have made it possible for health providers to monitor a patient's health remotely using actuators, sensors, and other mobile communication devices" [14]. "The IoT-MD provides an environment where a patient's vital parameters get transmitted by medical devices via a gateway onto secure cloud based platforms where it is stored, aggregated and analyzed" [6]. Internet of Healthy Things (IoHT) – this classification includes wearable devices such as watches and clothing particularly for home health monitoring, as well as any device that can capture vital sign parameters such as the mattress or the steering wheel of your car [5]. The transmission and capture of vital sign patient data can be particularly useful in preventing hospital readmissions and providing feedback for chronic illness sufferers. It includes devices that remind the patient to take medication, as well as those for promoting healthier and more active lifestyles which can be highly beneficial. This includes biometric data continuously collected - not just traditional monitoring devices, but also exercise devices, IoT shorts, mattresses, in fact anything that can hold a sensor.

Clearly these definitions are not discrete and can be overlapping. Hence companies such as CISCO are already redefining IoT to be the Internet of Everything (IoE) [15].

Benefits

It is suggested that healthcare will be the biggest beneficiary of IoT [16]. The real time monitoring of vital signs and conditions, as well as activity and compliance with prescribed treatments are two of the benefits of HIoT. Medications management is a huge burden to healthcare, both in terms of patient safety and in terms of cost. HIoT may help in better managing these costs using for instance, RFID tracking and the development of "smart" drugs with technology embedded into the medication itself [12, 17]. However, perhaps of more significance is "leveraged high-performance computing to provide real-time feedback and use evidence-based medicine to better patient outcomes" leading to improved patient care [6]. Further, evidence indicates that billions of dollars can be saved in healthcare costs by streamlining and sharing health data using HIoT for asthma management [12], and for other chronic disease management [2]. Flexible and remote patient monitoring is another example where cost savings can be found particularly when this prevents hospital readmissions [12], and by providing real-time disease management to improve patient outcomes. The influence on patient behaviour is seen as a benefit, empowering patients to be more involved in their own well-being [2].

III. The HIoT challenges and addressing them

The challenges are multiple and interconnected. They relate to the regulatory environment of healthcare, medical device manufacture, connectivity, interoperability, integration, device vulnerability, as well as privacy and security.

1) Regulatory medical device environment

The current regulatory environment surrounding traditional medical devices means that adopting new models of persistent data generation may be a difficult journey given the current timelines from production to implementation and use. The range of devices together with the necessity for trusted and reliable connection are critical to this technology uptake. The increasing connectedness and the reduced delineation of organizational boundaries pose information security concerns.

978-1-5090-4130-5/16/$31.00 ©2016 IEEE

2) Technical Debt

There are inherent problems, summarized as "the technical debt" from medical device engineering design, due to the lack of consideration of cyber security threats. This results in compromised medical devices with associated unpredictable behaviour [18]. The major concern is the impact of an exploitation rather than the exploitation itself.

3) Dynamic connectivity

HIoT is not a new computing platform, but a new way of using the existing architecture, bringing new security problems and challenges. The issue of dynamic versus static connectivity, with no fixed end points means that many of the usual communication mechanisms for transferring messages securely will not work. It is the global nature of the connectivity between devices that is the major security concern. The networks and connections over which data is travelling are often disparate and inconsistent and under the control of many different stakeholders. This means that there are significant challenges in the privacy and governance of this data, as well as its protection and security. At present these connections are highly reliant on trust.

4) Device diversity and interoperability

The truly interoperable HIoT system where data is both transferred one-to-one and one-to-many connections, incorporating exchange of data across multiple interfaces, will require systems to "play nice" with one another [19]. This is essential when you consider that in any data exchange between multiple systems, the combination of interfaces is 2(n-1). Whilst an issue for IoT in general, the ability for each device and exchange point to understand multiple transmission and security protocols is particularly relevant in healthcare. This is compounded further by the need to understand what code systems and terminologies are used with each device. There is no central registry of device capability. This informational representation even using standards, has proven to be difficult in the real world environment with existing data exchange capability [19]. Device management will require directories of devices functionality, protocols, terminologies and standards compliance. The level of "plug and play" interoperability now commonplace in non-health areas, is a long way off in the medical device arena.

5) Consistency and data integration

The integration of device-collected data into electronic medical record systems has significant development ahead of it to ensure the integrity of data and subsequently patient safety. Patient identification is one essential component where information is collected from multiple disparate devices and integrated into electronic record systems. In addition, data provenance - where the origin of data received from external systems needs to be established - is required to ensure data quality and authenticity of the information. One resolution for this is using unique device identification (UDI) for non-implantable healthcare devices and other consumer devices and Software as a Medical Device (SaMD) applications. Cross-border data transfer also requires special consideration particularly in relation to local regulation and legislation, for instance adherence to the Australian Privacy Principles [20]. Missing or incorrect data delivered into clinical information systems and EMRs will impact data integrity and is often particularly difficult to identify in the EMR itself [21].

Some of the issues are boundary condition related resulting from ill-considered or misunderstood integration of legacy systems as well as analogue to digital systems [18]. These issues create indirect security weaknesses. Further, the ability to collect data using HIoT in situations or locations that have previously not been accessible, for instance using Smart wearable clothing, and to provide appropriate and relevant healthcare support will mean that rigorous security, safety and privacy protocols will need to be in place, particularly where such systems are to be taken to scale and become part of normal routine care [17].

6) Privacy

Since many devices collect personal identifiable information, including health information, the privacy concerns are compounded when this data is being shared between mobile applications and cloud services connected to the device. The consistent lack of encryption, network misconfiguration, lack of knowledge on what security to implement, and the inability for the device to handle encryption, are some of the reasons for significant privacy concerns. That is not to say that the protection of confidentiality of data, and the subsequent impact on personal privacy has not always been present but in a HIoT world potential vulnerabilities are more difficult to identify as well as mitigate. Whilst the solution to data privacy is often implemented using policy-based access controls to data, this is complex and potentially impossible using an HIoT network, where control of individual devices is not within one organisation but shared between cooperating organizations.

An increasing threat to privacy is the ability to collate and cross-link information about individuals from various sources including IoT devices, and draw conclusions from this data. For example, linking geographical location with purchases from pharmacies may provide a profile of an individual's health status - linking doctors visited (from the geolocation data) with specialist qualifications may give further detail.

7) Security

Most security challenges are linked to the context of use, and whilst not specific to healthcare, rely on three elements. Firstly, data availability and ensuring consistent connectivity and access to services. Disruption to network functionality and denial of service attacks can have a major impact on healthcare delivery. Unlike the business sector, the impact is not restricted to reputation, financial loss and customer dissatisfaction, but may also affect patient safety where connections are critical. Further, a common defence-in-depth security measure is redundancy (duplication of devices/equipment, ready to be swapped into a network), however in healthcare this redundancy is not necessarily practical when the devices are life critical monitors or implanted devices.

Secondly, authentication and identity management to ensure encryption of data in transit, and sufficient authorisation and authentication measures. Many cloud and mobile technologies fail to require sufficiently complex passwords, and this is a serious cause for concern [11].

978-1-5090-4130-5/16/$31.00 ©2016 IEEE

Thirdly, system integrity through security protection mechanisms such as verification, monitoring and auditing, is vital. In a similar manner to the use of "bring your own device" (BYOD), IoT and its many derivatives were developing before a commonly accepted security framework and standards to address security were available. Indeed, there is little consensus on how to implement IoT security at the device, network or system levels [22]. A significant part of HIoT protection is knowing what is connected and what it is connected to. Recognition of potential security incidents is problematic because of the number and complexity of the potential vulnerability. This issue can be addressed by using secure services (SOA modelling) and an end-to-end IoT service [23].

The vulnerability to hacking devices like wearables and other embedded sensors, is compounded by a lack of regulatory oversight and safety standards in their manufacture [24], and by search engines e.g. Shodan, allowing searching for any Internet connected device and to explore the Internet of Things [25].

Many of the device related issues can be handled at the design and development phase of manufacture using new international standards for safety of such as the revision to IEC 62304 *Medical device software -- Software life cycle processes* and ISO/IEC 82304-1 *Health Software –Part 1: General requirements for product safety* (ISO/IEC 82304). Ultimately, to address the security and privacy issues, these must be implemented across the information systems and the organisation, which may require both technical and cultural change [26, 27].

8) Device vulnerability

The overall management of HIoT is another aspect to be addressed by organizations. It is already difficult to update the hundreds of medical devices in situ in clinical environments [28]. This is more complex with the software versioning and legacy operating systems used in the majority of medical devices [29]. The problem will grow as more devices are connected. A further complication will be vulnerabilities from default access credentialing on many devices, and the increasingly common web-based interface access [7]. The problems often occur where we have changed from static connectivity to dynamic connectivity. For instance, healthcare direct messaging is achieved through secure message delivery (SMD) [30]. However, to be efficiently and effectively deployed these current methods use an Endpoint Location Services (ELS), which enables discovery of the messaging endpoints and endpoint capabilities. This type of service will not function effectively using HIoT together with existing mechanisms. Similarly, traditional endpoint security where the transmission channels and the endpoints are known, and discoverable, is disrupted with the dynamic nature of HIoT.

Another issue is the difficulty of detecting computer-based infections affecting on devices. With minimal or no user interface, this detection together with what methods can be employed to debug security incidents, can be problematic [29]. A further problem may be the use of different telecommunications providers who are legally bound to provide information to law enforcement upon request. This may impact the adoption and use of the technology where patients are concerned about privacy, and potentially where "personal health and safety systems will become the next ransom-ware goldmine" [31].

Whilst the use of existing security measures can be effective to a certain extent, some of these are impractical for use with HIoT devices and applications. The limited storage capacities together with the low power consumption requirements of most devices means that techniques such as encryption will potentially need to be re-engineered to be effective security solutions. At present relying on security basics and employing defence-in-depth (a multilayered security approach) is a sensible option. Secure start-up, access control, device authentication, packet inspection capabilities (firewalls), and timely patching (software updates) are required as a minimum to ensure intended functional safety.

Security cannot be considered an add-on to an application, system, or now, device. Building security into the design of any device that has the potential to become part of the HIoT is essential. Internationally, where medical devices and health software are concerned, standards making bodies such as the International Organisation for Standardization (ISO) are revising and developing standards for the healthcare industry to incorporate the changing environment. These include such standards as ISO/IEC 82304 and the major revision of the ISO 80001 *Application of risk management for IT networks incorporating medical devices* series. A key concern in the application of standards such as ISO 80001 is that there is a need to profile each standard to particular organizational needs, which is often not well understood and most e-health professionals have little experience with such implementation.

9) Clinical workflow

There are inherent risks in using technology such as HIoT where patients may view data without an associated correct understanding of what the data means clinically. There is a need for diagnosis to still include the clinician regardless of alert conditions and automated decision support systems [6]. The major problem to be solved is the triage and management of data within clinical workflow. This problem has already been identified in the construction of remote patient and mobile monitoring [32], and will continue to be problematic in the short-term with HIoT.

a) Integration and use impacting patient safety

What needs careful consideration is the integration of devices, monitoring, alarms and their impact on patient safety. Fatalities from incorrect alarm settings on ventilators are an example of this, and remote surgical procedures using robotic surgery are a high risk activity when considering the network and internet enabled infrastructure required [21]. The stress from alarm fatigue is a well-recognized problem for patient safety. The increasing number of HIoT devices with potentially incorrect sensitivity levels will increase "alarm fatigue" for healthcare providers. This will become a substantial issue as more devices are deployed in home care and hospital environments [21, 33]. Similarly, there are multiple cases where differing sensing systems and subsequent automated population of the EMR have confused coding systems resulting in patient safety incidents [33]. Of greater concern is whether

978-1-5090-4130-5/16/$31.00 ©2016 IEEE

access to alarm systems and device interfaces are adequately controlled, and whether appropriate access to, and oversight of, configuration parameters to set tolerance and sensitivity levels is available.

IV. Discussion

There is no single solution to the security and patient safety issues arising from the Health Internet of Things. User education on best security practice is required as well as awareness of the HIoT challenges. The use of, and conformance to, security standards is necessary by device manufacturers, communications and application developers, as well as implementation and integration specialists.

Whilst part of the solution lies in creating standards to guide HIoT development and use, many of the current standards need to be updated to work in this new IoT environment. At present it is essential to adapt the effective security controls, developed over many years, to the unique constraints of HIoT and to the embedded technology that future networks will comprise [22]. The practical approach to risk assessment currently used will need to be revisited and risk decisions re-evaluated in light of HIoT [7]. As noted by Williams and Woodward [29] the integration of medical devices in the same way as the adoption of HIoT, will require a holistic approach to assessment of security risk and vulnerability mitigation. The new composition of networks means that every device in connection may represent a potential risk and provide access to other parts of the interconnected network and devices.

V. Conclusion

This paper identifies the challenges for security and the impact on interoperability in the healthcare setting of HIoT. Consequently, a deeper systematic analysis based on a formalised security and privacy ontology, such as the HL7 Version 3 Standard: Security and Privacy Ontology [34] would assist further work in this area.

Technological developments are bombarding healthcare faster than healthcare can make clinical use of them. There is no doubt that the ability to manage remotely networked and automated devices to support patient care and healthy living, will be of benefit to healthcare. However, the move from static to dynamic networks and from closed enterprise networks to publicly accessible mobile Internet connections presents many security dilemmas. In the same manner that security should be an enabler of healthcare data exchange, it is also a foundational element to enable HIoT.

This is a new paradigm for healthcare. Is it possible to deliver safe and effective healthcare, at a distance and independent of time and location? This extends the existing bounds of telemedicine: it shifts the involvement (however passive) of the patient and explores data gathering on a massive scale to better assess 'normal' in a public health and cohort sense, and personalized to what is 'normal' for an individual.

The balance between reducing cost of care and potentially improving patient outcomes, weighed against patient privacy, data confidentiality and cyber security threats, may be a pivotal factor in the widespread adoption of HIoT. Further, the lack of standardization across the sector in terms of device, software and terminology capability and interoperability, will hinder this adoption and subsequent widespread use in the short-term. However, in the longer term, if workflow, data triage, and efficient processes to harness the data are developed, then HIoT does have the ability to revolutionize healthcare. The complex nature of the integration of devices and demanding interoperability requirements means that the healthcare environment stakeholders must use established standards for communication, interoperability and semantic understanding. In such a diverse setting establishing trust for information collection, sharing and use will be essential. The platforms for this already exist using HL7 v2, CDA and FHIR, as well as ISO design and safety standards. These coupled with IHE data exchange profiles, and terminologies including SNOMED, LOINC, OpenEHR and ICD-10, will go a long way to ensuring consistency. This will also demand however, that manufacturers, developers, and vendors all cooperate to create true interoperability and lessen the requirements for proprietary solutions, along with a commitment to ongoing investment in maintaining terminology translation maps Ultimately, HIoT will be both transformational and disruptive, but the question of whether the potential for HIoT to reduce healthcare costs and provide better patient care will outweigh the security implications of volumes of data on clinical workflow, remain unanswered. However, these benefits in collaboration with cloud technologies and the capabilities of big data may well be the way of the future, if not already happening now. If cyberattacks and the threat environment are not addressed now, HIoT will become another attack vector to compromise vulnerable devices and systems.

We must learn from the mistakes of the past: design of devices for seamless interconnection, must ensure that best security practice, hardening of systems and secure protocols are inherent in these devices. The challenge is creating end-to-end security solutions that can incorporate the security of individual devices as well as the network and information system as a whole. This is currently a major challenge for the healthcare sector and will no doubt become more complex using HIoT.

Whilst the consumer push for engagement of the health profession with monitoring devices will grow, we must not lose sight of the overall aim to improve healthcare whilst ensuring patient safety. The transfer of clinical data and the potential for new sources of data collection is enormous. Whilst this data may be useful for future big data analysis, the challenge in triaging this data from a clinical perspective, is not yet solved.

Cybersecurity and the threat environment is moving faster than policy and regulation. However, the way forward in protection for HIoT will be new standards to address the use of the connected architecture and devices together with increased oversight and regulation by industry and government.

References

[1] J. Moar. (2015). *Smart wireless devices and the Internet of Me* [Online]. Available: http://www.juniperresearch.com/document-library/white-papers/smart-wireless-devices-internet-of-me

978-1-5090-4130-5/16/$31.00 ©2016 IEEE

[2] S. Kramer. (2015). *How the Internet of Things will impact healthcare* [Online]. Available: https://powermore.dell.com/technology/how-the-internet-of-things-will-impact-health-care

[3] Markets and Markets. (2015) *IoT Healthcare Market by Components - Global Forecast to 2020* [Online]. Available: http://www.researchandmarkets.com/research/g6n36x/iot_healthcare

[4] T. J. McCue. (2015). *$117 billion market for Internet of things in healthcare by 2020* [Online]. Available: http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#58d793712471

[5] J. Kvedar. (2016). *Harnessing the Internet of health things* [Online]. Available: http://www.himssasiapac.org/sites/default/files/HIMSSAP_ThematicReport_HarnessingtheInternetofHealthThings.pdf

[6] A. Khanna and P. Misra. (2014). *The Internet of Things for medical devices - Prospects, challenges and the way forward* [Online]. Available: http://www.tcs.com/SiteCollectionDocuments/White%20Papers/Internet-of-Things-Medical-Devices_0714-2.pdf

[7] ISACA. (2015). *Internet of things: risk and value considerations* [Online]. Available: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-value-considerations.aspx

[8] E. Kovacs. (2015, 24 July 2015). *Fiat Chrysler Recalls 1.4 Million Cars Following Jeep Hack* [Online]. Available: http://www.securityweek.com/fiat-chrysler-recalls-14-million-cars-following-jeep-hack

[9] A. Greenberg and K. Zetter. (2015). *How the Internet of Things Got Hacked* [Online]. Available: http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/

[10] FDA, "Cybersecurity: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," Federal Drug Administration ,2015.

[11] Hewlett Packard. (2015). *Internet of things research study 6* [Online]. Available: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

[12] B. Harpham. (2015). *How the Internet of Things is changing healthcare and transportation* [Online]. Available: CIO. http://www.cio.com/article/2981481/healthcare/how-the-internet-of-things-is-changing-healthcare-and-transportation.html

[13] TechTarget. (2015). *IoMT (Internet of Medical Things)* [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

[14] S. Fluin. (2016). *The Medical Internet of Things* [Online]. Available: http://mobcon.com/medical-internet-things/

[15] CISCO. (2013). *Internet of Everything (IoE) value index* [Online]. Available: http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf

[16] EY. (2015). *Cybersecurity and the Internet of Things* [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

[17] S. Miles. (2014). *The Internet of Medical Things* [Online]. Available: http://news.mit.edu/2014/internet-medical-things?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq

[18] K. Fu. (2015). *On the technical debt of medical device security* [Online]. Available: http://cra.org/ccc/wp-content/uploads/sites/2/2015/11/Kevin-Fu-Medical-Device-Security.pdf

[19] SourceMedia. (2016). *Interoperability: Why systems needs to play together* [Online]. Available: http://www.healthdatamanagement.com/whitepaper/why-systems-need-to-play-together

[20] Office of the Australian Information Commissioner. (2012). *Australian Privacy Principles* [Online]. Available: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

[21] ECRI Institute, *Top 10 health technology hazards for 2015*. 2014.

[22] Wind River. (2015). *Security in the Internet of Things* [Online]. Available: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[23] GSMA. (2016). *GSMA IoT Security Guidelines Overview* [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.11-v1.1.pdf

[24] J. I. Wong. (2016). *Cybercrime is booming and the Internet of Things will just make things worse* [Online]. Available: http://qz.com/603996/cybercrime-is-booming-and-the-internet-of-things-will-just-make-things-worse/

[25] Shodan. (2016). *Shodan: the search engine for <everything>* [Online]. Available: https://www.shodan.io/

[26] L. Coles-Kemp, J. Reddington, and P. A. H. Williams, "Looking at clouds from both sides: The advantages and disadvantages of placing personal narratives in the cloud," *Inform. Security Tech. Rep.*, vol. 16, pp. 115-122, 2011.

[27] L. Coles-Kemp and P.A.H. Williams, "Changing Places: The Need to Change the Start Point for Information Security Design," *Electron. J. Health Informatics*, vol. 8, p. e13, 2014.

[28] B. Schnier. (2014). *The Internet of Things Is Wildly Insecure — And Often Unpatchable* [Online]. Available: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

[29] P.A.H. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices: Evidence and Research*, vol. 8, pp. 305-316, 2015.

[30] *AS 5552-2013 E-health secure message delivery*. Australian Standard, 2013.

[31] C. Daly. (2014). *Interview with Bob Bigman, Former CISO of CIA* [Online]. Available: http://www.activecyber.net/interview-with-bob-bigman-former-ciso-of-cia/

[32] P. A. H. Williams and A. J. Maeder, "A conceptual framework for secure use of mobile health," *J. Int. Soc. Telemedicine and eHealth*, vol. 1, pp. 44-51, 2013.

[33] ECRI Institute, *Top 10 patient safety concerns for healthcare organisations 2015.* 2015.

[34] *HL7 Version 3 Standard: Security and Privacy Ontology, release 1,* HL7 Standard, 2014.

978-1-5090-4130-5/16/$31.00 ©2016 IEEE