The Contemporary Ethical and privacy Issues of Smart Medical fields

Victor Chang, Yujie Shi and Yan Zhang
International Business School Suzhou
Xi'an Jiaotong-Liverpool University, Suzhou, China
Email: victorchang.research@gmail.com

Abstract

With the development of big data technology, such as data mining and data matching, many industries have started a revolution, including medical field. Big data not only strengthens the accuracy of medical diagnosis, but it also enhances the efficiency of the entire medical system and relevant medical staff. Additionally, with the rethinking of innovation, the application of wearable intelligent device, Radio-frequency identification (RFID) technology and sensor technology play positive roles in promoting medical interaction between hospital system and wearer. Smart medical provides effective methods for individual health management and promotes the progress of medical information. However, there are also some inevitable ethical problems, e.g., the leakage of privacy information, which cannot be avoided to some extents. We recommend a list of good data processing and handling practices to reduce the possibilities of ethical problems happened during the data flow process.

1. Introduction

With the rapid growth of the network and technology in recent years, the speed and quantity of digital data have been produced increasingly and rapidly. So far, all industries are actively involved in big data applications, and the smart healthcare industry has no exception. Big data has the potential to offer more health services for individuals and populations, since it can be more cost-effective for healthcare operations and can lead to new treatments for chronic and infectious diseases. Big data has brought a great impact

on the development of the traditional medical industry, from the traditional paper records to electronic health records, to improve the efficiency and accuracy of the medical treatments. The popularity of wearable devices and smart home care systems has not only improved the emergency response of healthcare systems but it has also raised awareness on health monitoring. The widespread use of RFID technology and sensor technology can enhance the quality and safety of pharmaceuticals and medical devices. However, due to the large and complex data in the field of medical industry, big data has greatly challenged the development of the medical industry. At the same time, it has posed great challenges to technology, social system and informal system such as ethics. Based on the existing research, this article summarizes the issues of morality, ethics and privacy in the field of smart medicine under the influence of big data and puts forward some suggestions.

2. Literature review

As the "new oil" in the 21st century, big data has become a hot topic in all walks of life. People have realized that big data can offer great opportunities in various fields such as commerce, healthcare and government. However, there are different versions of big data definitions. Big data can be defined as "relative terms" (Minelli et al., 2013) to describe the rapid development of computer technology and the dramatic increase in data volume (Albrecht and Fangerau, 2015). In the dialectical way of thinking, the definition of big data has four main aspects: a) Some scholars focus on the attributes of data, including the size, speed and diversity of data in order to highlight the novelty of big data (Laney, 2001). b) Other scholars focus their attention on the entire process, focusing on the collection, management and use of data. That is, data found through data processing (Boyd and Crawford, 2011). c) Of course, some scholars have also focused their attention on big data, especially on exploring the limitations of big data. In particular, Boyd and Crawford (2011) consider big data to describe the ability of businesses or individuals to collect, organize and use large databases. d) On the basis of the first three points of perception, some scholars have focused their attention on the socio-economic, cultural and political conditions underlying the phenomenon of big data (Ekbia et al., 2015). IBM does not define in that particular way, but rather in terms of quantity, breed, speed, and accuracy (IBM, 2017).

Although there is no unified definition of big data presently, it has been widely used in the modern society and has provided massive opportunities for the development in all

fields. Therefore, many problems have emerged in the introduction of new technologies in different sectors. In particular, in addition to the various laws, regulations and policies, emerging issues such as ethics should be carefully evaluated, since it has direct impacts on the society and people. The issues of ethics and big data depend largely on how we define ethics (Herschel and Miori, 2017). In fact, the study of ethical issues began 2400 years ago, since there were mainly four kinds of views: Kant's ethics, Bentham and Mill's utilitarianism, Rousseau and Locke's social contract theory, Dodd and Plato's moral ethics(Herschel and Miori, 2017). Using these four theories to explain big data, Kant's theory describes that everyone should follow a rule or a code of ethics that states that everyone's information can or cannot be shared is obviously impossible, and Kant's Theory is only suitable as a moral basis for big data analysis (Kantian ethics, 2016). Utilitarianism shows that assessing the ethics of big data from a practical point of view is complicated because it requires the quantifying the consequences of using big data and its services. In other words, by analyzing the consequences of all the related people involved, we can understand the implications and meanings behind. Obviously, such analytical methods are not only complicated, but they also have many uncertainties, such as deviation analysis, inaccurate measurement and several others (Quinn, 2016). Social contract theory emphasizes that rational people will agree to be bound by the contract, because as long as everyone abides by the rules, they are for the benefit of all (Herschel and Miori, 2017). However, different societies have different rules. In the United States, for example, different laws are applied to different departments. In the EU, data protection is a fundamental right they are trying to implement (Scott, 2016). In particular, the theory of social contract requires rational people to work together to determine the scope of big data. The application of big data in this aspect is morally correct, and it is beneficial to the community as a whole. Virtual ethics focus on the character of the performer and their suitability, that is to say, people must evaluate who uses big data and their intentions and behaviors(Herschel and Miori, 2017). This means that virtue ethics requires people to carefully examine individual behaviors to determine whether such behaviors meet the moral requirements.

In 2009, the concept of "Smart Planet" was born in the American Business Leaders Roundtable（Holzinger etc. al., 2015). In China, the concept of "Smart Healthcare", "Smart Transportation," "Smarter Supply Chain," "Smarter Power," "Smarter Agriculture," and "Smarter Bank" to work together can form the practical concrete area of Smart Earth.

Prior to this, countries all over the world have gradually started to involve the smart medical businesses. For example, the Swedish Medical Center, Hannover Medical School in Germany, the University of Pittsburgh Medical Center and other agencies through the computer technology innovation, can make the medical operation efficiency to be improved significantly (IBM, 2016). In 2015, the concept of "Internet +" and Healthy China was first proposed (Assuli, 2015). With the wide spread of information technology, the medical industry is increasingly keen to start building electronic files and health information exchange system (Patty et al., 2016). By moving from a paper-based system to a digital system, the healthcare industry has started to advocate the sharing of medical information. The popularity of GPS-enabled mobile applications and tracking / wearable devices, in particular, not only offers tremendous opportunities to improve healthcare systems and healthcare, but it also addresses geographical inequalities while increasing productivity (Patty et al., 2016). Although smart healthcare has brought rapid positive changes to the health care industry, it has also brought great challenges. Assuli (2015) said that the proliferation of electronic files also poses huge demands on data security and the issue of patient privacy also raises the issue of citizens' privacy violations. Some scholars believed not only expressed concerns about the security of data analysis methods and databases, but they also said that medical data sharing can also raise citizens 'thinking about how to control personal information and how the government supervises data respecting citizens' personal information (Patty et al., 2016). At the same time, Albrecht and Fangerau (2015) believe that database developers or related technical staff are not clear about data confidentiality and the scope of the use of restrictions. Information technologies such as data matching and data mining make the data available at will. It not only raises patients' concerns about the privacy of the medical environment but it also reiterates widespread concerns about the collection, use and disclosure of data and the need for personal information, sensitive information, and health information Concerns about privacy and confidentiality (Rajaretnam, 2014).

3. Smart medical fields and big data

In fact, as long as patient-related data is generated, a variety of data-based digital medicine can be generated. In other words, healthcare professionals can use the patient's health information as a basis to monitor changes and make recommendations for the patient's treatment, care, or health. However, as a general rule, the data used by

healthcare workers is a one-time paper medical record that is not only limited in scope but stored in a specific institution that cannot be shared (Assuli, 2015). Healthcare organizations have embarked on smarter healthcare by introducing various digital technologies that can transform incomplete and confusing paper data into fast, exhaustive digital data.

These technologies are considered as branches of Internet of Things (IoT) technologies, including RFID technology, sensor technology, positioning technology, nanotechnology, physical marking technology, video recognition technology, intelligent embedded technology and other intelligent sensing technologies (Guo et al., 2016). With these technologies, people can not only effectively collect information such as people, medicines and equipment, but also process, store or share information. Among them, RFID technology has significantly improved the service level of the medical industry. In particular, RFID technology can not only prevent counterfeit medicines from being produced and sold, ensure the quality of medicines during the manufacture of medicines, but it also can be used by the construction of hospitals or urban medical systems for optimization of service procedures and reduction of consultation time (Patty et al., 2016). Cloud computing is mainly used for smart medical management, including medical information storage, data management (Li and Chen, 2014). At the same time, the proliferation of smart devices facilitates the timely monitoring of information, allowing healthcare facilities to monitor patients' health, behaviors and location at any time using digital technology, particularly the GPS positioning systems (Lupton, 2015).

Therefore, the establishment of medical information-based system can enhance the accuracy of medical diagnosis and improve the efficiency of medical staff and the entire medical system. For citizens, the proliferation of smart medical technologies allows them to better monitor their own health and to have access to a better medical assistance through telemedicine (Holzinger et al., 2015). For the government, the establishment of a smart healthcare system has enabled the government to deal more effectively with the control of certain infectious diseases (Lupton, 2015). At the same time, it is undeniable that technological advances have promoted the development of personalized medicine.

4. The privacy and ethical issues of smart medical fields

It has been found that a large number of rapid and exhaustive data are continuously emerging in various fields. Businesses analyze the data they collect to get the information

they need, use the data as a basis for management and regard data analysis tools as a management medium. At the same time, the widespread use of technology inevitably leads to some ethical issues. Ethics is a tool to identify and justify good and acceptable behavior(Kitchin, 2016). Before discussing ethical issues in the context of health care, interactions between doctors and patients and between medical devices and the pharmaceutical industry have taken place. As a result, different ethical issues have arisen in the process of data collection, management, regulation and sharing.

- Privacy

Privacy refers to the individual's rights to limit the extent to which others know individual information and the extent to which others obtain personal information(Milica and Bart De, 2016). In other words, privacy is the individual's right to individually demonstrate to the community (Kitchin, 2016). In general, when people put aside the law to explain or understand privacy, privacy mainly refers to accepting and disclosing the acceptability of personal information, including sensitive information. In the medical field, we summarize the form of privacy in this way. It mainly includes identity privacy, health privacy, location and mobile privacy (Rajaretnam, 2014).

The uniqueness of the medical field determines that the creation of a medical record means that personal and even sensitive information (such as genetic information) is being collected and that individuals do not know that personal information (including sensitive information) about them is being collected and how they are used. In today's healthcare industry, electronic health records and health information exchange networks are already in use (Assuli, 2015). Electronic health records include all previous medical information, such as previous surgery records, hospitalization information, and individual drug sensitivities. Clearly, the proliferation of electronic health records prevents double testing and reduces the healthcare costs of switching between different medical facilities or medical devices (Assuli, 2015). Compared with paper medical records, the benefits of electronic medical records can overcome unreadable handwriting or data obfuscation problems (Rajaretnam, 2014). However, when the medical field relies on electronic devices or new technologies to gather information, it means not only the privacy and sensitivity of the medical records can be a concern but also risks of identity frauds and other problems may arise, when the mobile devices are lost or the technology loopholes happen. Often this may lead to accidental disclosure of information (Lupton and Lupton, 2016). In particular, if the health care providers use the patient's medical records directly as the

basis for making the diagnosis, and if the data are not collected at this time and the doctor is not aware of the situation, then the diagnosis may have a great impact on the accuracy and validity.

When medical specialists collect personal data using electronic records, wearable devices and other technologies, people gradually lose control of the data. Especially, organizations that obtain the data, and do not need informed consent when repackaging the data for re-sale and reuse, but the information owners do not know that their data has been used to know what the purpose (Kitchin, 2016). Obviously, if all information is treated as secret or shared, it is unrealistic to be completely open or completely private (King& Richard, 2014). The second application of medical and health information refers to the application of personal health information beyond the scope of direct medical services, mainly including the analysis and research of diseases, the evaluation of the quality of health services, the research on health policies and business activities (Assuli, 2015). The second use of medical information, such as re-screening important information directly from the health repository, has the advantage of being efficient, accurate and rapid. Obviously, the second use of information at the same time face the risk of leakage of information again. However, some countries did a good job of protecting the secondary use of medical information, especially in the United Kingdom and Canada. The United Kingdom and Canada have set a good example for countries all over the world in using medical information for the second time and can effectively prevent the issue of information disclosure. In Canada's medical information re-use service system, the agency responsible for the collection needs to be program certified for information and the researcher has to go through three steps to get the information it needs(Wang, 2015). The purpose of this approach is to minimize the disclosure of information and maximize the use of information.

In addition to being reuse, the collected data may also be sold by certain agencies or individuals for a special purpose, and the individual information owner does not know it at this time. Data buyers use the data they purchase to analyze people's daily lives, not only to make basic analyzes and judgments about people's information, but also to predict what they can do in the future(Rajaretnam, 2014). In fact, there are many such examples in real life. In February 2016, Shanghai Pudong Court ruled that two staff members from Shanghai CDC stole 200,000 newborn babies in Shanghai and sold them to infant and baby product management companies (Yuan,2016). At this point, personal information is

no longer using medical and disease treatment, but also by the use of business. In particular, when we talk about insurance, people are worried about whether insurers differentiate their products if the insurer gets information from the hospitals, which could damage people's interests(Milica and Bart De, 2016).

- Security

Security is a prerequisite for protecting the privacy of patients. The importance of the confidentiality of medical information is to protect individuals against other discrimination and shame of information disclosure(Assuli, 2015). Therefore, in the field of smart medical security, mainly refers to the safety of information, that is to say, the safety of personal medical electronic documents, including information storage security, information dissemination security. Especially in the era of the rapid development of digital technology, electronic medical records gradually replace paper medical records, presenting a great challenge to the security of data storage and access (Zhao et al., 2016). As the medical field contains too much sensitive information, at the same time, it also places high demands on the security in the process of data dissemination.

In the medical field, enterprises, medical institutions or researchers mainly collect data through electronic medical records, wearable devices and smart home care systems. Obviously, these digital approaches make it easier to collect data and improve diagnostic efficiency(Milica and Bart De, 2016). At the same time, however, this means that health care workers have free access to personal medical records without express permission, and the owner of the information is unaware of the situation (Assuli, 2015). For medical staff, there is a cognitive bias as to which information belongs to the patient's privacy information. There are still many healthcare professionals who believe that some medical information about a patient is not covered by privacy (Ou and Lan, 2016).

In reality, the data breaches of the personal data information of medical institutions and developers are very common, including that generated by health and medical APPs (Albrecht and Fangerau, 2015). According to a recent report by the Bollywood Institute for Data Risk Independence, the cost of remediation of medical information leaks is highest, and the situation is deteriorating year by year. The Polanyi Institute staff said in a 2015 study on Data Disclosure Costs that the average cost of healthcare information disclosure worldwide was $ 363 compared to $ 398 in the United States (Liebowitz, 2015). In 2016, Russian hackers leaked the confidential medical records of U.S. Olympic athletes, which have caused great repercussions from all over the world (Herschel and Miori, 2017).

The leaked data show that some athletes use banned medications to obtain exemptions, including Olympic gold medalists. However, the athletes mentioned that their medical records were leaked without permission and could only be taken as prescribed. This information leakage has caused great damage to the athlete's reputation. In particular, a database of personal health and medical details has become the target of cybercriminals, who often use the information to benefit from theft and extortion(Lupton and Lupton, 2016).

- Re-Identification

Anonymization is one of the key strategies to ensure personal privacy. In the process of enterprise data collection using data mining techniques, although it may consider using anonymous technology to avoid individual information leakage, there are still some problems when enterprises use different databases to analyze data (Nunan and Di Domenico, 2013). For example, researchers can leverage public information and photos on Facebook and match the information of anonymous individuals on major dating sites with facial recognition software(Lupton, 2015). In the area of smart healthcare, Nunan and Di Domenico (2013) find that anonymous identification does not make a big difference in the U.S. medical services because using modern analytics to trace anonymous health information back to the individual, while the desensitized message goes through, the processed sensitive information can still be identified after matching the information in different databases. Therefore, when enterprises are using digital technology to analyze personal medical information, once the common information between different information is found in the information obtained by technologies such as data mining, the possibility of random connection increases. Obviously, the result of this is beyond people's expectations, big data analytics can not only get private information, but also generate unexpected random connections(Herschel and Miori, 2017). In particular, when it comes to genetic databases, the most sensitive part of healthcare, DNA is the only hallmark of every individual because DNA is different from traditional health data and DNA-based genetic information cannot be completely anonymous.

- Notice and Consent

In real life, people use a lot of smart technologies every day, and each technology generates its own data. Due to the sheer volume of data and the diversity of data, it is apparently unrealistic for individuals to monitor the use of all data. There are user protocols that need to be read even before certain technologies are used, but these

protocols are effectively non-negotiable or agree to denial of service(Patty et al., 2016). Moreover, more informed consent is also included in the entire exemption, which also deprives individual's rights to choose. Therefore, before facing the reality of adopting many new technologies, individuals all hope that it is impossible for them to make their own choices. In fact, informed consent is not a new term in the field of medicine, but the situation with informed consent becomes more complicated with the advent of the era of smart medical care. Informed consent is the process by which patients understand the disease, treatment, research options, and options that are either accepted or rejected (Guo et al., 2016). At present, with the popularization of electronic medical records, the promotion of the concept of medical information sharing and the widespread application of telemedicine in the treatment process mean that patient data can be used not only for a single treatment or research, but also for storage in medical institutions, research institutions and businesses, while government databases are available for future research (Albrecht and Fangerau, 2015). In the United States, a legacy expert has been brought to court for allegedly using DNA samples of Latin American tribes without their knowledge (Rajaretnam, 2014). As a result of the trial, the researchers paid the compensation, while Latin American tribes also said they launched the study. Obviously, if the researcher informs the information owner before each use of data, which avoids unnecessary hassles but at the same time increases the workload of the entire process. Therefore, in real life, it is not possible to inform the owner of the information about the purpose of use.

5. Recasting smart medical field

It is undeniable that the application of some new technologies such as data mining and data matching to the medical field does raise some ethical and ethical problems, especially due to the particularity of the medical field, which contains too much privacy information. Although it is difficult to determine a specific boundary about the ethical issues of smart healthcare, at its most basic level, there must be mutual respect and trust between the health care provider and the patient (Rajaretnam, 2014). Additionally, the authors make recommendations based on the data flow process, with the goal of reducing the likelihood of ethical issues occurring at every step possible.

The first step in data flow is data collection. In addition to using data mining and other Internet of things technologies to collect data during data collection, data analysts also need to use data source technologies to mark data and record the source and transport

process. Secondly, in the process of data collection, it is necessary to explicitly inform the information owner of the purpose of data usage, to avoid the use of data beyond the owner's expectations(Kitchin, 2016). In particular, the government needs to set up special departments to supervise and even enforce the joint participation of citizens and enterprises in data regulation(Patty et al., 2016).

The second process is data processing. In data analysis, data analysts must 'de-identify' the data and influence the privacy of individuals must be removed. For example, when data analysts use K-anonymity, I-Diversity, T-closeness and other anonymous protection technology, at the same time need to avoid different databases can be anti-recognition (Zhao et al., 2016). In the medical field, medical data can often be used multiple times or even repeatedly for some research. Therefore, many countries can draw on the secondary data of medical data in the United Kingdom and Canada for the second use of medical data which adapts to the development of their own country(Wang, 2015).

When it comes to data dissemination, healthcare organizations can leverage data encryption technologies such as the DES key encryption algorithm and RSA public key encryption algorithm in data encryption algorithms to encrypt the results of data analysis with the goal of preventing unauthorized organization / personal theft, tampering with the results (Zhao et al., 2016). In particular, adhere to the principle of informed consent when medical information is shared, and medical institutions or researchers inform the owner of the information.

The last process is data invasion. It is important to prevent companies from spying their users’ personal life, infringing on one's private realm and family life, and adversely affecting their chances of education, employment and insurance after analyzing data, which can exacerbate social inequity. Therefore, in terms of law, the government should formulate a complete set of laws and regulations concerning the medical field, in which the purpose is mainly to protect all aspects related to personal privacy. In particular, the government should establish clear penalties for the phenomena that companies use to manipulate people's behavior through data analysis in order to avoid such phenomena(Herschel and Miori, 2017).

6. Conclusion

Studying the impact of smart healthcare on ethical problems and privacy is an extremely complex task. This is due to the fact that electronic health records are vital to

modern medical treatments, with the sharing of medical information, any special and latest medical condition can be analyzed and studied by medical specialists. However, those data may be misused by people, especially some private medical information that information owners do not want to be known by others, and we do not know what the purpose these data will be utilized. Since it is infeasible and unlikely to solve the ethical issues and privacy totally, we should do our best to reduce the likelihood of ethical problems before, during and after using any data.

References

Albrecht, U.-V. & Fangerau, H. (2015). Do Ethics Need to Be Adapted to mHealth? A Plea for Developing a Consistent Framework. *World Medical Journal,* 61**,** 72-75.

Anonymous. *What is Big Data Analytics?* [Online].Available from: https://www.ibm.com/analytics/hadoop/big-data-analytics (Accessed: 29 November 2017).

Anonymous. *Smart medical solutions* [Online].Available from: http://www.doc88.com/p-1744328621568.html (Accessed: 29 November 2017).

Anonymous. (2016) *Kantian ethics* [Online].Available from: http://www.csus.edu/indiv/g/gskilld/ethics/kantian%20ethics.htm (Accessed: 29 November 2017).

Assuli, B. (2015). Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments. *HEALTH POLICY,* 119**,** 287-297.

Ekbia, H., Mattioli, M., Kouper, I., Arave, G., Ghazinejad, A., Bowman, T., Suri, V. R., Tsou, A., Weingart, S. & Sugimoto, C. R. (2015). Big data, bigger dilemmas: A critical review. *Journal of the Association for Information Science & Technology,* 66**,** 1523-1545.

Guo, W., Wang, J., Jing, W.-l. & Qian, H. (2016). 智慧医疗发展应用及其对策 / Development and Application of Wisdom Medical and Its Countermeasures. *医学信息学杂志 / Journal of Medical Intelligence***,** 1.

Herschel, R. & Miori, V. M. (2017). Ethics & Big Data. *Technology in Society,* 49**,** 31-36.

Holzinger, etc. al., (2015)'from smart health to Smart Hospitals', *Smart Health*, pp.1-20.

King, J. H. & Richards, N, M. (2014) What's up with Big Data ethics?[Online].Available from: http://www.forbes.com/sites/oreillymedia/2014/03/28/whats-up-with-big-data-ethics/ #2f6f8e012964 (Accessed 29 November 2017).

Kitchin, R. (2016). The ethics of smart cities and urban science. *PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A-MATHEMATICAL PHYSICAL AND ENGINEERING SCIENCES,* 374.

Laney, D. (2001). 3D data management: Controlling data volume, velocity, and variety. Retrieved from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Li, W.-j. & Chen, R. (2014). 基于物联网技术的智慧医疗系统及其建设策略研究 / Intelligent Medical System Based on the Internet of Things and Strategy Research of Its Construction. *激光杂志 / Laser Journal***,** 56.

Liebowitz, J. (2015) *Big data and business analytics*. Beijing, Tsinghua University Press.

Lupton, D. (2015). Health promotion in the digital era: a critical commentary. *HEALTH PROMOTION INTERNATIONAL,* 30**,** 174-183.

Lupton, D. & Lupton, D. (2016). Digitised health, medicine and risk. *HEALTH RISK & SOCIETY,* 17**,** 473-476.

Milica, M. & Bart De, D. (2016). Ethical aspects in eHealth – design of a privacy-friendly system. *Journal of Information, Communication and Ethics in Society***,** 49.

Minelli, M., Chambers, M. & Dhiraj, A. 2013. *Big data, big analytics. [electronic resource] : emerging business intelligence and analytic trends for today's businesses*, Hoboken, N.J. : John Wiley & Sons, Inc., 2013.

Nunan, D. & Di Domenico, M. (2013). Market research and the ethics of big data. *International Journal of Market Research,* 55**,** 2-13.

Ou, S.-l. & Lan, X.-x. (2016). 患者隐私权保护中非正式制度缺漏与补遗--基于智慧医疗条件下的实证调查研究 / On the Informal Institution Gaps and Addendum in the Protection of Patients´ Right of Privacy. *浙江万里学院学报 / Journal of Zhejiang Wanli University***,** 38.

Patty, e., Helen, e., Simon ede, L., Edward, e., Ben, e., Graham, e., Phil, e., Peter, e., Corinne, e., Rachel, e., Emma, e., Angela, e., Ralph, e., Sarah, e., Raquel, e., Olivia, e. & John, e. (2016). Who Owns The Data? Open Data for health care. *Frontiers in Public Health, Vol 4 (2016)*.

Quinn, M. J. 2016. *Ethics for the information age*, Boston : Pearson, [2016] 7th edition.

Rajaretnam, T. (2014). DATA MINING AND DATA MATCHING: REGULATORY AND ETHICAL CONSIDERATIONS RELATING TO PRIVACY AND CONFIDENTIALITY IN MEDICAL DATA. *Journal of International Commercial Law & Technology,* 9**,** 294-310.

Scott, M. (2016) U.S. and Europe in 'Safe Harbor' data deal, but legal fight may await [Online]. Available from: http://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html?_r=0 (Accessed: 29 November 2017).

Wang, Y.-f. (2015). 医疗健康信息二次利用中安全隐私保护. *医学信息 / Medical Information***,** 269.

Yuan, Y. (2016) *Medical big data solution to health problems of the three major pain points* [Online].Available from: http://insurance.hexun.com/2016-09-07/185904302.html (Accessed 29 November 2017).

Zhao, H.-q., Jiang, Q. & Zhao, W. (2016). 大数据学习分析的安全与隐私保护研究 / Research on Security and Privacy Protection of Big Data Learning Analytics. *现代教育技术 / Modern Educational Technology***,** 5.