PacificMUN

Dare to Speak

IBC-Topic A

Backgrounder Guide

Privacy Issues of Collecting Informationfor big data projects - IBC

Topic A

PacificMUN

Letter from the Director

Dear delegates,

My name is Jessica Lin and I have the utmost pleasure of serving as the Director of the International Bioethics Committee 2019. I am currently a grade 11 student at Crofton House School and it has been four years since I stepped foot into my first committee room. Although I hardly raised my placard during my first conference, Model UN has not only allowed me to grow as a public speaker, but it has also given me the opportunity to discuss some of the most pertinent issues in the world with like-minded individuals. I hope that this conference, and Model UN as a whole, has the ability to do the same for you.

With the widespread development of new biomedical technology and its practices gaining traction, many of the ethical implications have yet to be addressed internationally. In this committee, we will be discussing the issues surrounding the advancing biological research field, specifically the Privacy Issues of Collecting Information for Big Data Projects and the Right of Choice for Unresponsive Patients. It is important to understand that bioethics is not a field that supplies absolute answers; the solutions you seek may evolve as quickly as the biomedical sector itself. While these topics may be challenging, research and reflection will greatly aid your understanding, and help you formulate both your own and your country's stance on these topics.

On behalf of your Chairs, Alexander Shojania and Jesse Hsieh, the dais team is excited to witness a weekend of lively debate and fruitful discussion in February. Many thanks to Harrison Chan for writing the Topic A backgrounder. In the meantime, please direct any questions regarding the committee, topics, or the backgrounder to ibc@pacificmun.org.

Best regards,

Jessica Lin
Director of IBC
PacificMUN 2019

Committee Overview

With the rapid developments in the medical and life science field within the last half century, many medical breakthroughs have occurred, yet a fair share of unethical behaviour have also occurred. The United Nations Educational, Scientific and Cultural Organization (UNESCO) therefore formed the Bioethics Programme to address the cultural, social, legal, and ethical implications brought forth by these developments.

Specifically within the Bioethics Programme, the International Bioethics Committee was formed in 1993 by the General Director of UNESCO, Dr. Federico Mayor Zaragoza. Comprised of a body of independent experts from various countries gathered to discuss legal and ethical issues involved in the application of life science. As the only international forum for reflection in bioethics, this body ensures human dignity and freedom is respected in the progress made in the life sciences field. In 1998, as part of the Statues of the International Bioethics Committee, the Intergovernmental Bioethics Committee (IGBC) was created. This body of 36 Member States and their representatives meet at least once every two years to discuss the advice and recommendations placed forward by the IBC, and reports back to the IBC with opinions and proposals.

To ensure the healthy natural evolution of the human, care needs to be taken to prevent unsafe, unethical, or immoral practices from occurring, especially through the oversight of the IBC. The implementation of further regulation for the ethical development of medication and technology is important, and as such the IBC is tasked with the mitigation of risks of medical exploration and usage of recently developed medical practices and medication. This mitigation of risks helps to ensure the safety and freedom of humanity while continuing to allow research into the human body to continue.

Through this committee, many ethical and moral issues will be discussed around how to prevent unethical usage of data, as well as the question of unresponsive patients.

Topic Introduction

The development of modern computing technologies has revolutionized data collection, storage and movement. Within the realms of healthcare, this has translated into digitizing patient healthcare records, as well as storage on the “cloud,” enabling the sharing of such information between the patient, healthcare providers and insurance companies. Furthermore, development of the Internet of Things (IoT) has led to the creation of devices such as connected health trackers, apps and wearables, for example, the Fitbit which generate a multitude of metrics related to healthcare, such as fitness activity, sleep patterns, heart rate patterns. These metrics are then stored in servers around the world and processed through algorithms to generate usable information. In addition, many websites are also able to generate information for research. For example, Google can generate data based off one’s search history and interactions with health-related websites. Facebook and other social media posts can also help develop trends in a certain user’s health, as posts can be analyzed for tone and feelings, which can show mental health and wellness indicators. In turn, these trends in data can be prepared and sold off to third parties, thus monetizing

While the accessibility of records and the processing of data are advanced, cloud storage and digitization opens vulnerabilities to hackers and unwanted access, for example the 2015 Anthem Blue Cross data breach, where the personal details of nearly 79 million people were hacked and exposed. To hackers, this data is extremely valuable and can be used for illicit fraudulent activities.

Today, researchers have begun using the collected medical data in order to improve the general health level of the public. Some of the data collection and analysis can yield results such as the monitoring of diseases, healthcare management, medical device usage, clinical practice improvement and research. Furthermore, some believe that the cure to cancer is also held in the big data collection and analysis. However, the mass collection of data also includes many privacy issues that needs to be addressed.

Timeline

1972 - The Regenstrief Institute develops the world’s first electronic medical record system.

1990 - The Internet in its current form, the World Wide Web was developed and launched.

1996 - The Health Insurance Portability and Accountability Act was introduced in the US.

1997 - Latanya Sweeney, a graduate student successfully re-identified Massachusetts Governor Weld's hospital visit history using an health insurance database and a voter's list.

2006 - New York Times reporters successfully re-identify individuals from an anonymous AOL database of user search queries.

2013 - Fitbit releases the first Fitbit worn on a wrist, tracking movement and sleep patterns.

2014 - Apple released HealthKit, an all-round health informatics system.

2015 - Anthem Blue Cross, an insurance provider, was hacked into, affecting nearly 79 million.

Historical Analysis

With the exponential growth of the World Wide Web enabling access to a wide variety of services, ensuring the privacy of data collected has been a contentious and important issue given the significance of some of the data. Some of the most important data collected is healthcare data. Healthcare data will continue to be created in increasing amounts as most countries transition to a fully electronic medical record system.

Some countries have attempted to combat the problem surrounding the expectation of healthcare data privacy by defining different classes of information, notably "Personally Identifiable Information" (PII), and in the US additionally, "Protected Health Information" (PHI). These classes of information include items such as name, address, identification numbers (passport, SIN, credit card, etc.) The countries that have defined these classes of data have regulations regarding protection of these information- specifically requiring that this data be removed or "stripped" when being shared or used for medical research and big data purposes. However, many large countries by population, for example China, still does not have regulations protecting the privacy of the subjects and their data.

Furthermore, the United States had implemented the Health Insurance Portability and Accountability Act, known as HIPAA. HIPAA implemented stringent regulations on the protection of PHI, creating lasting effects on how data security on servers is implemented in the US in order for healthcare providers to remain HIPAA compliant. This bill did positively increase data security for healthcare related data and patient information, but it also affected research negatively. The University of Michigan reported that after HIPAA, completion of follow-up surveys completed by heart attack patients dropped from 96.4 percent to 34 percent, as well as having incremental costs associated with ensuring the survey remained HIPAA compliant. As part of HIPAA, if consent is not obtained, then a certain amount of personal identifiers must be removed from the data in the study.

The use of an electronic medical record system exacerbates the problem as data is more easily shared with researchers. In addition, the new developments in DNA sequencing technology also increases the concerns regarding privacy. The falling cost and speed of human genome sequencing only widens the availability for researchers to access genome data, which reveals data regarding age, gender, as well as pre-existing conditions and diseases. For example, current US regulations permit healthcare providers to provide a patient's genome to whomever requests, including researchers. Furthermore, some states permit researchers to legally obtain blood no longer used for a patient's care, then sequence the genome and add the information to a database, without the patient's consent or permission. In fact, gene sequencing in research is often times executed without the consent of the person's DNA being sequenced. Genome sequencing is important in the context of privacy as well- in addition to revealing age, gender and conditions, the genes also carry indicators and markers that can indicate and identify ethnicity makeup, as well as family lineage when compared to a database. While genes cannot completely re-identify its owner, it can eliminate most samples within a gene pool and identify close matches.

Therefore, the concerns regarding healthcare data privacy are largely caused by the way Electronic Health Records work, in addition to the regulations of countries and also current norms for the practice of healthcare research.

Current Situation

Globally, there is no current international standard regarding healthcare data. While certain countries and entities have placed regulations protecting the privacy of healthcare data, most countries' health data security and privacy have no regulation and are extremely autonomous. Many research organizations in countries are free to take data from electronic records as desired.

However, for those countries that do have regulations, two current models of consent to research are widely used today. Firstly, a model of broad consent, widely accepted for use in the European Union. Broad consent is when a person consents to their information as well as other physical parts (such as blood or tissue) to be used for an area of research, and researchers working on research in a given area are free to use their information and genome. Conversely, the other model of consent, opt-out consent, assumes the subject has consented to their data being used for research purposes unless the user specifically opts out of this usage. This model requires healthcare practitioners to explain the research in a way that the subject can fully understand. Unfortunately, many times in cases of opt-out consent, the research is not explained and opt-out is not clear.

It is not a surprise then that the public does not seem to trust research and big data projects, as the motives of research are often obscure and vague. A survey conducted in 2007 by the Institute of Medicine in the United States revealed that only 69 percent of respondents would trust healthcare researchers with their data compared to 83 percent with healthcare providers. A further analysis of this survey reveals that a majority of respondents are worried about discrimination if the personally identifiable health information was revealed, displaying a link between privacy and potential discrimination, or links to other factors such as employment, insurance rates or government programs. Finally, 38 percent of respondents (a majority in this case), would like each research study to describe the study and collect individual, specific consent. This survey shows the public distrust for these programs and highlights issues with the current research practices, especially in needing transparency.

In addition, current ethics norms and regulation allow research when it has been “de-identified.” However, de-identification does not mean it is completely impossible to reconstruct and re-identify the subjects. For many years, a belief was held that removing names and identification numbers was sufficient in de-identifying data and eliminates the risk of harm being done. However, as datasets grow increasingly larger and algorithms become more powerful, it has become increasingly easy to match data and re-identify the owner. This is done by comparing multiple datasets and finding commonalities, then merging the data together. A case of this occurring was in 1997 by a MIT graduate student, Latanya Sweeney. The Massachusetts government had made de-identified insurance claim records public, and by merging the data with a voter’s list, was able to pick out then-Governor Weld’s history of medical visits. Furthermore, in 2001, Sweeney was able to match anonymous Washington health records with voter data 43 percent of the time. In the current era, algorithms exist to re-identify patients with information about their prescriptions.

Furthermore, another problem is the untraceable secondary usage of data. In healthcare provider collected data, the primary usage of healthcare information can be controlled to a certain extent, such as researchers leveraging a specific dataset such as an ideal situation where the patient gives consent for their data to be used in a specific research project. However, most data in research ends up being uploaded to a large database, that are shared by many researchers and institutions. For example, US government funded research projects mandate data to be uploaded to a national database. However, once this data reaches the database, it is hard to trace where that data will be reused, and the original patient will have no knowledge even though they may have consented to the initial use.

Another type of data is the trends collected by websites, such as search engines, health tracking apps and social media platforms. These user-generated data are often overlooked but play a massive role in the generation of healthcare metrics through the traceability of user behaviour. For example, searching about a particular symptom on a search engine would generate data for that engine, which would then feed information about that behaviour to a third-party advertiser. Therefore, user behaviour is traceable and is tied to the user through their name, IP address and other traceable internet metadata. Likewise to Internet tracking, pharmacies have been known to sell de-identified data to pharmaceutical companies.

In summary, much of the current situation regarding this topic relates to the handling of research data. The sharing of data with third parties is a rampant issue and poses a big privacy risk and could allow de-identified data to be re-identified.

United Nations Involvement

The United Nations has several general publications and resolutions on data management and privacy, discussing in general the need for privacy. However, one of the most significant is from the International Bioethics Committee, which published a report, “Report of the IBC on Big Data and Health” in 2017 with a section specifically dedicated to ethics regarding research and another on privacy and confidentiality. This section also acknowledges the weaknesses of de-identifying information, as well as the knowledge that the public knows they have lack of control over their personal data.

Seeking Resolution

In generating possible solutions, it is important to acknowledge the benefits and drawbacks of each specific solution, in addition to referring to previous attempts' mistakes. Furthermore, it is also helpful to recognize the fact the IBC is only an advisory body and has no regulatory powers. Given the diversity of healthcare research using big data and its limitless applications, no singular approach will suffice and the question of prioritizing individual privacy over research (individual vs. society) will arise, and as a country, it would be beneficial to take a stance and be prepared to defend it.

Establish worldwide common privacy guidelines

This ambitious project would see the UN work in creating a guideline specifically regarding the treatment and handling of medical data. For countries that do not have set regulations regarding medical data, this could be an influential first step in ensuring countries respect the privacy of individuals. However, it is important to note that this would possibly interfere with nations that have established regulations on data protection, as well as would be near impossible to enforce as the IBC.

Individual ownership and storage of healthcare data

Proposals have been made to shift the way electronic health data are stored. One particular proposal is to shift the storage from the healthcare provider and their servers to the user. By allowing the user to "own" their data, they can choose who and which projects to share their information and data with. However, a potential drawback may be that users would be reluctant to share their data- leading in a smaller data pool for researchers to work with and possibly hindering research efforts.

Awareness of Public on Data Usage

Many surveys have pointed out that the general public are unaware of the purpose behind the usage of their personal information, or even that their healthcare data is often being used without their consent. By improving the general public awareness about this, the patient would ideally have more knowledge about their individual rights regarding their data, as well as actions that they can take to prevent unethical data usage and protect their privacy. By educating the public about the purpose of research, this solution hopes to restore trust in research. The increasing of public awareness however, is not and should not be a full solution to the problem, but rather one of the methods to help the current situation.

Bloc Positions

While these blocs are roughly based off of economic status, other blocs are also viable in the context of this topic. Consider your country's membership in geopolitical unions, for example the African Union and BRICS, and the actions that they have taken towards healthcare. Consider the culture and attitudes towards healthcare in your countries, as well as what kind of health system is used.

Developed Countries

Developed countries such as the US, Canada, Australia, and the EU have established electronic health record systems and are in the process of fully converting to EHR. These countries serve as an example of how EHR can be deployed and adopted in medical sector. Having had a long history of using EHR, these countries have stringent regulations surrounding the usage of data in medical research. For these countries, a task would be finding ways to balance privacy regulations and ethics with the ability to conduct research. In addition to a full rollout of EHR in these countries, another viable goal for these countries would be to improve upon the current models of EHR such as migrating towards user-based data storage.

Emerging Countries/Markets

Many emerging countries characteristically have a high population, coupled with booming economic growth, and increasing influence. However, many of these countries are only beginning to implement electronic health records in healthcare systems or have yet to implement EHR. Also, medical research in these countries may not yet be very established. In addition, some emerging markets have inconsistent access to healthcare - only the wealthy or those who live in urban centres have access. Therefore, it is of importance to work towards the integration of security in establishing electronic systems while these countries are still developing the EHR systems. Due to the extremely large population in these emerging markets and their growth, analysts have projected that emerging markets will become the forefront of digital health record developments.

Developing Countries

These countries are least likely to have developed some form of electronic healthcare infrastructure, as many of their healthcare systems are still developing and often times in need of aid. For these countries, there often is a lack of political stability, leading to an unstable healthcare system. Therefore, one of the largest concerns for these countries is to establish a working healthcare system. Furthermore, resources are often constrained in these countries, and the situation is quite problematic. In many situations, neither the patient nor practitioner is aware of healthcare rights and responsibilities, and literacy rates are low, so the patient might have a hard time understanding of their rights. However, in these countries, privacy matters the most, as some cultural norms have not yet developed to accept people with different medical conditions, for example HIV or mental health.

Discussion Questions

1. Should patient privacy be prioritized over data usability in research?
2. Will increased transparency in research practices help mitigate privacy concerns regarding the use of data?
3. Is it necessary to restore the trust of the general population in healthcare researchers?
4. What can be done to help regulate secondary usage of healthcare data?
5. Should the monetization of healthcare data, information and trends be allowed?
6. How do we mitigate the risks of data re-identification?
7. How can the IBC advocate for proper privacy in research data?

Further Reading

https://catalyst.nejm.org/big-data-healthcare/

https://www.practicalbioethics.org/what-is-bioethics

https://www.sciencedirect.com/science/article/pii/S1877050917317015

https://www.wired.com/2014/11/on-sharing-your-medical-info/

https://academic.oup.com/jlb/article/4/1/94/2910475

https://www.nytimes.com/2017/01/02/opinion/the-health-data-conundrum.html?_r=0

Bibliography

Patil, Harsh Kupwade, and Ravi Seshadri. "Big Data Security and Privacy Issues in Healthcare." 2014
IEEE International Congress on Big Data, 2014, doi:10.1109/bigdata.congress.2014.112, https://www.researchgate.net/publication/282280458_Big_Data_Security_and_Privacy_Issues_in_Healthcare.

Faggella, Daniel. "Where Healthcare's Big Data Actually Comes From -." Tech Emergence, 11 Jan. 2018, www.techemergence.com/where-healthcares-big-data-actually-comes-from/.

"Investigator's Guide to HIPAA." Research Affairs, researchaffairs.llu.edu/responsible-research/human-studies/hipaa/investigators-guide-to-hipaa.

"Healthcare Data as a Public Good: Privacy and Security." *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary*, but Claudia Grossmann, National Academies Press, 2010, http://www.ncbi.nlm.nih.gov/books/NBK54293/.

"Medical privacy and security in developing countries and emergency situations." *Privacy International*, London School of Economics, March 2012, http://privacyinternational.org/sites/default/files/2017-12/Privacy_International_Medical_Privacy.pdf

"The Digital Healthcare Leap." *Digital Health in Emerging Markets*, PwC, February 2017, https://www.pwc.com/gx/en/issues/high-growth-markets/assets/the-digital-healthcare-leap.pdf.

"EMR: The Progress to 100% Electronic Medical Records." *The University of Scranton Online*, 30 Aug. 2018, https://elearning.scranton.edu/resourcec/health-human-service/emr_the-progress-to-100-percent-electronic-medical-records.

Sharma, Rahul. "What is PII and PHI? Why is it Important?" *FileCloud*, March 2, 2015, https://www.getfilecloud.com/blog/2015/03/what-is-pii-and-phi-why-is-it-important/#.W8QVThNKglL.

Zhang Luxia, Wang Haibo, Li Quanzheng, ZhaoMing-Hui, Zhang Qi-Min. Big data and medical research in China *BMJ* 2018; 360 :j5910, doi: https://doi.org/10.1136/bmj-j5910 (Published 05 February 2018)

Kuzubek, Jim. “The Limits of Big Data in Medical Research.” *Scientific American*, 3 April, 2018, https://blogs.scientificamerican.com/observations/the-limits-of-big-data-in-medical-research/.

Meyer, Michelle. “Reidentification as Basic Science (Re-Identification Symposium).” *Petrie-Flom Center at Harvard Law School*, 26, May, 2013, https://blogs.harvard.edu/billofhealth/2013/05/26/reidentification-as-basic-science/.

Kulynych, Jennifer. “Is Privacy the Price of Precision Medicine?” *Oxford University Press*, 26 March, 2017, https://blog.oup.com/2017/03/privacy-precision-medicine/.

Kulynych, Jennifer, and Henry T. Greely. “Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research When Privacy and Science Collide | Journal of Law and the Biosciences | Oxford Academic.” *OUP Academic*, Oxford University Press, 15 Jan. 2017, https://academic.oup.com/jlb/article/4/1/94/2910475.

“Report of the IBC on Big Data and Health.” *UNESCO Digital Library*, UNESCO, SHS/YES/IBC-24/17/3, REV. 2, Paris, 15 September, 2017, http://unesdoc.unesco.org/images/0024/002487/248724e.pdf.

Armstrong D, Kline-Rogers E, Jani SM, et al. Potential Impact on the HIPAA Privacy Rule on Data Collection in a Registry of Patients with Acute Coronary Syndrome. *Arch Intern Med*. 2005;165(10):1125–1129. doi:10.1001/archinte.165.10.1125, https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/486568/

Appari, Ajit, and M. Eric Johnson, “Information Security and Privacy in Healthcare: Current State of Research.” *Center of Digital Studies*, Tuck School of Business, Dartmouth College, August 2008, http://www.ists.dartmouth.edu/library/416.pdf

“International Bioethics Committee.” *UNESCO*, http://www.unesco.org/new/en/social-and-human-

sciences/themes/bioethics/international-bioethics-committee/.