ETHICAL, LEGAL AND SOCIAL ISSUES ARISING FROM BIG DATA AND ARTIFICIAL INTELLIGENCE USE IN HUMAN BIOMEDICAL RESEARCH

A CONSULTATION PAPER

BIOETHICS ADVISORY COMMITTEE

SINGAPORE

May 2023

BIG DATA AND ARTIFICIAL INTELLIGENCE REVIEW GROUP

Chair
Professor Patrick Tan Boon Ooi
Professor, Cancer and Stem Cell Biology Programme, Duke-NUS Medical School;
Executive Director, Genome Institute of Singapore; and
Director, SingHealth Duke-NUS Institute of Precision Medicine (PRISM)

Co-Chair
Associate Professor Ngiam Kee Yuan
Group Chief Technology Officer, National University Health System; and
Senior Consultant, Division of Thyroid and Endocrine Surgery
National University Hospital and Alexandra Hospital

Professor Chin Jing Jih
Chairman, Medical Board
Senior Consultant, Department of Geriatric Medicine
Tan Tock Seng Hospital

Associate Professor Michael Dunn
Associate Professor and Director of Undergraduate Education
Centre for Biomedical Ethics
Yong Loo Lin School Medicine
National University of Singapore

Professor Kon Oi Lian
Adjunct Professor
Duke-NUS Medical School

Dr Pavitra Krishnaswamy
Senior Scientist and Principal Investigator, Machine Intellection Department
Deputy Head, Healthcare & MedTech Division
Institute for Infocomm Research
Agency for Science, Technology and Research

Professor Graeme Laurie (International Panel of Expert)
Professorial Fellow
School of Law
University of Edinburgh, Scotland

Emeritus Professor Lee Eng Hin
Emeritus Professor, Department of Orthopaedic Surgery
National University of Singapore; and
Emeritus Consultant
National University Hospital

Mr Charles Lim Aeng Cheng
Principal Senior State Counsel
Legislation Division
Attorney-General's Chambers

Professor Julian Savulescu
Chen Su Lan Centennial Professor in Medical Ethics
National University of Singapore;
Director, Centre for Biomedical Ethics
Yong Loo Lin School of Medicine
National University of Singapore; and
Uehiro Chair in Practical Ethics
University of Oxford, United Kingdom

Professor Tan Sor Hoon
Professor of Philosophy and Academic Director
School of Social Sciences
Singapore Management University

Mr Tan Sze Yao
Director, Legal Office
Ministry of Health, Singapore

Dr Voo Teck Chuan
Assistant Professor, Centre for Biomedical Ethics
Yong Loo Lin School of Medicine
National University of Singapore

Table of Contents

CHAPTER 1: FOREWORD

With advances in information technology, data and computational analytics in recent decades,[1] the use of big data[2] and AI[3] in human biomedical research is becoming increasingly important, enabling researchers and healthcare professionals to analyse massive datasets, generate useful insights, and enhance data-driven decisions. While the growing use of big data and AI in biomedical research promises benefits, it also raises ethical issues such as the need for protecting data privacy versus ensuring societal benefit; importance of obtaining informed consent and respecting individual's rights and autonomy; and the extent of data security obligations with respect to the value of data. These warrant further deliberation and review by the Bioethics Advisory Committee (BAC).

2 Recognising these ethical challenges, the BAC has developed a public consultation paper to discuss the ethical issues arising from the use of big data and AI in human biomedical research, such as responsible data usage, data ownership, custodianship, and stewardship, data privacy, accessibility and security, data anonymisation and other ethical considerations and issues specific to AI. The paper also covers the ethical principles to guide the ethical use of big data and AI applications in human biomedical research, such as respect for persons, solidarity, justice, proportionality, sustainability, and other ethical considerations including integrity, transparency, accountability, consistency and stakeholder engagement. The public consultation paper is an adapted version of the final advisory report.

3 The views of the public, stakeholders, research institutions, and interested organisations will assist the BAC in developing recommendations in the final advisory report to guide academics, researchers, healthcare professionals, Clinical Ethics Committees (CECs) and Institutional Review Boards (IRBs) on the ethical use of big data and AI applications in human biomedical research.

[1] Cremin, C. J., Dash, S., & Huang, X. (2022). Big Data: Historic Advances and Emerging Trends in Biomedical Research. *Current Research in Biotechnology*, *4*, 138–151. https://doi.org/10.1016/j.crbiot.2022.02.004

[2] Big data comprises massive amounts of data generated in the private and public sectors, and includes data from individual medical records, patient health records, results of medical examinations, data collected by using diagnostic and health management devices or applications as part of internet of things (IoTs), and data from electronic data sources such as web searches, forum posts and images.

[3] AI describes the use of computers and technology to simulate intelligent behaviour and critical thinking comparable to a human being.

CHAPTER 2: EXECUTIVE SUMMARY

The main topics covered in the Public Consultation Paper (adapted from the advisory report) include:

a. Responsible Data Usage

2 Responsible data usage ensures that data is used in a fair and transparent manner without compromising data integrity and seeks to protect individual privacy and control of personal data. It is also key to preventing risk of discrimination or injustice, or inaccurate research outcomes stemming from bias in AI algorithms and the data used to train the algorithms. Ethical principles of *justice, consistency, transparency* and *accountability* would be key considerations to guide researchers, institutions and IRBs on how human biomedical research data should be managed and used responsibly to avoid the risk of discrimination arising from participation or biases in biomedical research. The Chapter also discusses how researchers or developers should ensure that data fed into the algorithm is not biased or result in bias-driven outcomes when developing AI algorithms.

b. Data Ownership, Custodianship, and Stewardship

3 With increasing use of big data and AI in biomedical research, data owners need to ensure that the data is secured and appropriately accessed whereas data custodians ensure that mechanisms are in place to ensure the responsible and ethical use of data to protect the privacy of individual data, and data security. Data stewardship complements data custodianship by ensuring the safe management of the data resource and training and educating stakeholders about the importance of responsible data management. The Chapter discusses the application of ethical principles of *respect for persons, justice, accountability, proportionality, solidarity, consistency* and need for stakeholder engagement in examples of whether a person who had provided biological materials or data but had not participated in the subsequent processing or analysis should have intellectual property rights in the data, and how large volumes of biomedical data shared across countries in international research collaborations should be managed.

c. Data Privacy, Accessibility and Security

4 Data privacy, accessibility and security would be necessary to ensure that individuals' personal data rights and interests are protected through robust technical security systems while facilitating access to the protected data by legitimate third parties. The Chapter discusses how providers and researchers can ensure robust and proper access control while maintaining data privacy, and how institutions or organisations managing data stored in multiple on-site servers or cloud repositories can ensure appropriate data accessibility through the application of ethical principles and values of *respect for persons, solidarity, proportionality, integrity, transparency* and *accountability*.

d. Data Anonymisation, De- and Re-identification of Data

5 Anonymisation, de- and re-identification of data are tools used in biomedical research to enable data to be analysed while protecting the data contributors' privacy. As analyses involving big data and AI algorithms in biomedical research rely increasingly on large volumes of personal, health and medical data, conventional methods of de-identification and

anonymisation may no longer be adequate in protecting data privacy. The Chapter discusses how the risks of re-identification can be managed when linking data from multiple sources, and whether genetic data should be treated differently from other types of personal and health data through the application of ethical principles and values of *respect for persons, justice, consistency, solidarity, proportionality, and accountability.*

e. Revisiting Consent in the Arena of Big Data and AI

6 Consent could be classified as implied, broad, specific, explicit, and dynamic. Ethical considerations that should be considered when obtaining informed consent from research participants with respect to big data use include differences in consent taking for health and medical data collected via various sources versus novel data collection methods, and differences between consent for usage of data from cohort studies and that from real-world data. The Chapter discusses the application of ethical principles *respect for persons, justice, integrity, solidarity, proportionality,* and *sustainability* to guide researchers and institutions on how informed consent should be obtained for data derived from novel and emerging sources, whether waiver of consent should be allowed for the proposed research, and if specific or broad consent is appropriate for biomedical research involving personal information.

f. Responsibility to the Public in Data-Sharing for Research

7 Responsible data sharing can lead to research that benefits individuals, communities, and society. The challenge is in ensuring that data sharing for research is conducted ethically, equitably, and with proper respect for privacy. The Chapter discusses how the benefits of biomedical research can be shared with participants whose data is used through the application of ethical principles *solidarity* and *justice.*

g. Use and Storage of Legacy and Posthumous Data

8 Posthumous data pertaining to one's health and medical conditions may be donated and used for purposes of medical research which can provide significant benefits such as in the development of cures and treatments for diseases and medical conditions. Ethical principles to be considered when using and storing posthumous and legacy datasets include *respect for persons* and *sustainability.* The Chapter discusses how legacy and posthumous datasets can be used and stored ethically.

h. Ethical Considerations and Issues Specific to AI

9 The lack of clarity or consensus on ethical issues that apply to AI in biomedical research such as *transparency, explainability* and *justifiability* is a major concern. Other key considerations include adhering to best practices and standards to ensure reliability and safety, human agency and oversight, equitable access and model security to minimise potential harm to individuals and parties involved in research projects. The Chapter discusses on whom the responsibility should be attributed to for AI's wrong decisions, how equitable access to AI technologies can be ensured in research globally, and how a robust AI model security can be built.

The Executive Summary of recommendations will be included in the final advisory report.

CHAPTER 3: INTRODUCTION

This chapter defines big data and AI and highlights the global and local trends of big data and AI use in biomedical research and the corresponding ethical concerns. An overview of the objective and scope of the advisory report is also provided here.

Big Data

3.1 The concept of big data is not totally new but has become more popular in recent decades given advances in information technology, and data and computational analytics.[1] The origins of large data sets go back to the early 1960s and 1970s with the first data centres and development of relational databases. With the evolution of big data and technologies, the collection of information, documentation and analysis of data has markedly changed all aspects of personal and professional life, especially in areas of governance and resource management.[2]

3.2 Big data is commonly defined as information characterised by high volume, variety, and velocity.[3] Heterogenous variability, veracity, and value are additional factors which also characterise big data.[4, 5] In addition, big data consists of data collected from collaboration networks that cannot be managed, processed, analysed or understood by conventional methods or software and require specific computing technology and analytic methods.[6, 7] Today, big data comprises massive amounts of data generated in the private and public sectors, and includes data from individual medical records, patient health records, results of medical examinations, data collected by using diagnostic and health management devices or applications as part of internet of things (IoTs), and data from electronic data sources such as web searches, forum posts and images.[8]

3.3 The amount of big data generated increases every year, with a significant portion comprising data for biomedical research and healthcare obtained from analysing patient tissues, blood, body fluids and laboratory investigations from research institutions and clinical records alike.[9] Since 2011, Singapore's healthcare industry

[1] Cremin, C. J., Dash, S., & Huang, X. (2022). Big Data: Historic Advances and Emerging Trends in Biomedical Research. *Current Research in Biotechnology*, *4*, 138–151. https://doi.org/10.1016/j.crbiot.2022.02.004

[2] Fisher, C. K., Smith, A. M., & Walsh, J. R. (2019). Machine Learning for Comprehensive Forecasting of Alzheimer's Disease Progression. *Scientific Reports*, *9*(1). https://doi.org/10.1038/s41598-019-49656-2

[3] Sivarajah, U., Kamal, M. M., Irani, Z. *et al*. (2017). Critical Analysis of Big Data Challenges and Analytical Methods. *Journal of Business Research*, *70*, 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001

[4] Vogel, C., Zwolinsky, S., Griffiths, C. *et al*. (2019). A Delphi Study to Build Consensus on the Definition and Use of Big Data in Obesity Research. *International Journal of Obesity*, *43*(12), 2573–2586. https://doi.org/10.1038/s41366-018-0313-9

[5] Hashem, I. A., Yaqoob, I., Anuar, N. B. *et al*. (2015). The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues. *Information Systems*, *47*, 98–115. https://doi.org/10.1016/j.is.2014.07.006

[6] Dash, S., Shakyawar, S. K., Sharma, M. *et al*. (2019). Big Data in Healthcare: Management, Analysis and Future Prospects. *Journal of Big Data*, *6*(1), 54. https://doi.org/10.1186/s40537-019-0217-0

[7] Oussous, A., Benjelloun, F.-Z., Lahcen, A. A. *et al*. (2018). Big Data Technologies: A Survey. *Journal of King Saud University - Computer and Information Sciences*, *30*(4), 431–448. https://doi.org/10.1016/j.jksuci.2017.06.001

[8] Jiang, F., Jiang, Y., Zhi, H. *et al*. (2017). Artificial Intelligence in Healthcare: Past, Present and Future. *Stroke and Vascular Neurology*, *2*(4), 230–243. https://doi.org/10.1136/svn-2017-000101

[9] Garcia-Milian, R., Hersey, D., Vukmirovic, M. *et al*. (2018). Data Challenges of Biomedical Researchers in the Age of Omics. *PeerJ*, *6*, e5553. https://doi.org/10.7717/peerj.5553

has undergone transformative changes as Singapore ventured to establish the National Electronic Health Record (NEHR) system to centrally pool all patients' records such as medication and laboratory reports from different healthcare providers. Supporting the 'One Patient, One Health Record' directive, the NEHR has been steadily introduced to public and private healthcare institutions across Singapore and mandatory participation may be required from all healthcare institutions, subject to further reviews and announcement by the Ministry of Health (MOH), Singapore. Other than the clear benefits of giving healthcare professionals access to a patient's comprehensive health records, the implementation of the NEHR system also provides avenues for furthering biomedical research and enhanced analytics capabilities in disease-surveillance and population health research.[10] A well-managed and quality-controlled data infrastructure would also enhance Singapore's international reputation and make it more appealing as a research resource for biomedical researchers.

3.4 However, the challenges in managing and maintaining big data is considerable, especially in the context of biomedical research where data protection, privacy and security are paramount. Ensuring the confidentiality of the data is important, particularly in the use of personal data or anonymised data where there is risk of data re-identification. The understanding of concepts on data ownership, custodianship, and stewardship is also crucial to the management and use of big data in ensuring accessibility, security, quality and proper data governance. Other issues related to data quality, such as missing data, incorrect or incomplete data, and data inconsistencies, may also arise, which could impact the validity and reliability of research findings. This in turn, would result in biases introduced for predictive modelling or decision-making. Managing big data ethically in biomedical research requires careful ethical considerations and attention to the complexities and challenges involved, and appropriate policies, procedures/processes and measures should be considered and put in place to ensure the responsible collection, storage, analysis, and sharing of data, while safeguarding the privacy and confidentiality of individuals' information.

Artificial Intelligence

3.5 Artificial Intelligence (AI) describes the use of computers and technology to simulate intelligent behaviour and critical thinking comparable to a human being. The term, AI, was first described in 1956 as the science and engineering of making intelligent machines.[11] For instance, AI-driven analytic techniques are procedures used to enable computers to show human like intelligent activities such as visual perception, speech recognition, decision-making, natural language understanding. In the process of data analysis, AI automates the steps that humans would take to complete analysis, such as learning and reasoning and uses insights and patterns to make predictions about what drives outcomes and can even learn to improve its predictions over time. The main advantages of AI-driven analytic techniques are: (i) reduction of time taken to perform (big data) analytics; (ii) efficient execution of

[10] Bhandari, M. (2017). 'Is Data Singapore's Next Big Bet?'. *The Straits Times*. (2017, February 9). Retrieved December 12, 2022. http://www.straitstimes.com/opinion/is-data-spores-next-big-bet

[11] Amisha, Malik, P., Pathania, M. *et al*. (2019). Overview of Artificial Intelligence in Medicine. *Journal of Family Medicine and Primary Care, 8*(7), 2328. https://doi.org/10.4103/jfmpc.jfmpc_440_19

repetitive tasks via the help of machine learning; (iii) reduction of human errors; and (iv) enhancement of the degree of precision.[12]

3.6 A common application (and a subset) of AI is machine learning where algorithms are trained to identify and resolve patterns like the human brain.[13] A recent development of deep neural networks (a subset of machine learning) further imitates the human brain's ability to identify images, objects, improve drug discovery, upgrade precision medicines, improve diagnosis and assist humans to make decisions.[14]

3.7 AI has advanced biomedical research and healthcare globally. In 2021, Nvidia, one of the leading technology companies based in the US, launched Cambridge-1, currently the most powerful supercomputer in UK. Some of Cambridge-1's current partnerships include: (a) AstraZeneca to accelerate drug discovery using machine learning to discover new molecules for drugs or screen patients more quickly; (b) GlaxoSmithKline (GSK) to enhance predictive modelling by processing large complex data at new levels of speed, precision and speed; and (c) King's College London to train AI models to generate synthetic brain images by learning from Magnetic Resonance Imaging (MRI) brain scans to gain better understanding of diseases such as dementia, stroke, brain cancer and multiple sclerosis and enable earlier diagnosis and treatment.[15] In 2022, Nvidia, National Supercomputing Centre Singapore, National University Health System (NUHS) and SingHealth signed collaborations to build a supercomputing infrastructure, with Nvidia providing access to its software development kits, open-source pretrained AI models and high performance computing expertise to help accelerate biomedical research in Singapore.[16]

3.8 While the use of AI in biomedical research has the potential to improve our understanding of diseases, drug discovery, and personalised medicine, it also raises concerns and potential challenges including the transparency, explainability and justifiability of AI which need to be addressed. In addition, while there is a need for validation of AI algorithms to ensure that AI systems are accurate, reliable, and generalisable to different populations and contexts, this could be challenging in biomedical research, where the complexity and variability of data make it difficult to establish gold standards for validation. There are also concerns that the rapid development of AI in biomedical research could outpace ethical and legal frameworks, which highlights a need for ongoing discussion and development of ethical guidelines and regulations to ensure that AI is used in a responsible and ethical manner.

[12] Rahmani, A. M., Azhir, E., Ali, S. *et al*. (2021). Artificial Intelligence Approaches and Mechanisms for Big Data Analytics: A Systematic Study. *PeerJ Computer Science, 7*. https://doi.org/10.7717/peerj-cs.488

[13] Wiens, J., & Shenoy, E. S. (2017). Machine Learning for Healthcare: On the Verge of a Major Shift in Healthcare Epidemiology. *Clinical Infectious Diseases, 66*(1), 149–153. https://doi.org/10.1093/cid/cix731

[14] Davenport, T., & Kalakota, R. (2019). The Potential for Artificial Intelligence in Healthcare. *Future Healthcare Journal, 6*(2), 94–98. https://doi.org/10.7861/futurehosp.6-2-94

[15] NVIDIA. (2021). Nvidia Launches UK's Most Powerful Supercomputer, for Research in AI And Healthcare. *Nvidia Newsroom.* (2021, July 6). Retrieved December 12, 2022. https://nvidianews.nvidia.com/news/nvidia-launches-uks-most-powerful-supercomputer-for-research-in-ai-and-healthcare

[16] SingHealth. (2022). New Supercomputer to Speed Up Heart Disease, Future Pandemic Research. *SingHealth News.* (2022, March 2). Retrieved December 12, 2022. https://www.singhealth.com.sg/news/tomorrows-medicine/new-supercomputer-to-speed-up-heart-disease-future-pandemic-research

Relationship Between Big Data and AI

3.9 While big data and AI are distinct technologies with distinct uses, both work well together, and frequently rely on one another. The relationship between big data and AI is synergistic – while big data analytics leverages AI for better data analysis, AI systems require a massive scale of data to learn and improve decision-making processes.[17, 18] AI is futile without big data and mastering data is insurmountable without AI.

Global and Local Trends of Big Data and AI Use in Biomedical Research, Clinical Research and Healthcare

3.10 Traditionally, biomedical research has been conducted via hypothesis driven models to elucidate the mechanisms underlying diseases and to identify novel therapeutic targets and signalling pathways with possible drug targets. Although this classical approach continues to be used, the use of big data and AI technologies has enabled researchers to extract features and valuable insights from large datasets.[1] With the continual development of new algorithms to improve accuracy in pattern recognition such as diagnosis and prediction of disease outcomes, big data and AI will play increasingly larger roles in the future of biomedical research, clinical research and healthcare.[19]

3.11 A mapping study done in 2019 on the research trends for big data analytics and AI in biomedical research, clinical research and healthcare reported that there was interest in developing AI for (a) medical image processing and analysis; (b) clinical decision-support; (c) physiological signal processing and analysis; and (d) healthcare operations. The most significant clinical specialties with application of big data analytics and AI were reported to be (a) oncology; (b) neurology; (c) cardiology; (d) pulmonology; and (e) radiology.[20] Examples of current use of big data and AI in biomedical and clinical research include:

a. European Research Infrastructure for biological data (ELIXIR), an intergovernmental organisation that provides resources across Europe, including databases, software tools, training materials, cloud storage and AI supercomputers which are supported and funded by the European Molecular Biology Laboratory (EMBL). ELIXIR's goal is to help researchers to capitalise on the huge amounts of big data produced in biomedical research to gain insights into health and disease.[21]

b. Global Alzheimer's Association Interactive Network (GAAIN) is the first operational online integrated research platform linking scientists with shared

[17] De Mauro, A., Greco, M., & Grimaldi, M. (2016). A Formal Definition of Big Data Based on its Essential Features. *Library Review, 65*(3), 122–135. https://doi.org/10.1108/lr-06-2015-0061

[18] Thapa, S. (2022). AI & Big Data: Understanding the Synergies. *Squadery.* Retrieved December 11, 2022. https://insights.squadery.com/ai-big-data-analytics-understanding-the-synergies/

[19] Ferretti, A., Ienca, M., Hurst, S. *et al*. (2020). Big Data, Biomedical Research, and Ethics Review: New Challenges for IRBs. *Ethics & Human Research, 42*(5), 17–28. https://doi.org/10.1002/eahr.500065

[20] Mehta, N., Pandit, A., & Shukla, S. (2019). Transforming Healthcare with Big Data Analytics and Artificial Intelligence: A Systematic Mapping Study. *Journal of Biomedical Informatics, 100*. https://doi.org/10.1016/j.jbi.2019.103311

[21] ELIXIR (2022). About Us. *ELIXIR-Europe.* Retrieved December 11, 2022. https://elixir-europe.org/about-us

data, and sophisticated analysis tools across a global network of Alzheimer's disease study centres. The GAAIN team recruits data partners and affiliates to perform comparative data analysis and cohort discovery to accelerate Alzheimer's disease research in a collaborative and innovative manner.[22]

c. Genomics Data Commons (GDC), a research programme funded by the US National Cancer Institute to provide the cancer research community with a unified repository and cancer knowledge base that enables data sharing across cancer genomic studies in support of precision medicine.[23]

d. Community Acquired Pneumonia and COVID-19 Artificial Intelligence (AI) Predictive Engine (CAPE), a local AI-enabled tool developed by Integrated Health Information Systems and Changi General Hospital that can predict the severity of pneumonia especially in COVID-infected patients, based on chest X-ray images. The AI predictive engine enables closer monitoring and treatment of patients with severe pneumonia for improved patient outcomes through timely triaging and treatment.[24]

Ethical Concerns

3.12 The use of big data and AI in biomedical research, clinical research and healthcare gives rise to ethical issues that warrant consideration and review. Some examples of potential ethical issues include:

a. Privacy vs societal benefit – The need to respect individuals is in tension with the principle of solidarity as the potential of big data research to benefit society is complicated by the imperative to protect privacy. In many cases, anonymisation and de-identification are either near impossible or akin to removing data that holds potential value for research.[25] Moreover, the degree of mutual obligation between individual and society needs to be considered and respected, especially in situations where participants may take on a disproportionate amount of risk and might be harmed when their data was made too widely available. In addition, the limitations on the extent of data privacy obligations for the use of anonymised data in multiple settings without the knowledge of the data subject need to be addressed. The potential from big data and AI is tremendous, but with this comes potentially increased risks to individual privacy. Considerable care is required to strike an acceptable and fair balance, moving forward.

[22] The Global Alzheimer's Association Interactive Network. (2022). *The Global Alzheimer's Association Interactive Network.* Retrieved December 11, 2022. https://gaain.org/

[23] National Cancer Institute (NCI) Genomic Data Commons (GDC). (2022). *NCI Genomic Data Commons.* Retrieved December 11, 2022. https://gdc.cancer.gov/

[24] Integrated Health Information Systems (IHiS). (2020). Artificial Intelligence Tool Developed to Predict Severity of Pneumonia in Patients, Including COVID-19 Patients. *Integrated Health Information Systems (IHiS).* (2020, October 1). Retrieved December 14, 2022. https://www.ihis.com.sg/Latest_News/Media_Releases/Pages/artificial-intelligence-tool-predict-severity-pneumonia-covid-patients.aspx

[25] Currie, J. (2013). 'Big Data' Versus 'Big Brother': On the Appropriate Use of Large-Scale Data Collections in Paediatrics. *Paediatrics, 131, Supplement,* S127–S132. https://doi.org/10.1542/peds.2013-0252c

b. Issues with informed consent – In traditional research, participants were informed about a specific research experiment and gave their informed consent for such a specific purpose, but this may be an impractical approach when it comes to big data research. In many cases of big data research, the attempt to secure informed consent might not be meaningful if the participants cannot be adequately informed. For example, Singapore's NEHR is immensely beneficial for the health database which would be extremely valuable for biomedical research but the financial, transactional costs, and impracticability of keeping to the traditional rules of informed consent (for researchers to approach each and every single person in this database for consent) would cripple efforts in utilising the database. The concept of 'reasonable limits' in researchers' and clinicians' ability to fully inform data subjects on the future use of their data needs to be considered since it may not be possible to obtain secure informed consent from participants at all times.

c. Problem with consent for decentralised data – Big data research often makes use of datasets that may not include participants' explicit consent to involvement in a specific research programme. This is evident with decentralised data[26], such as data gathered from social media platforms like Facebook and LinkedIn, wearables such as smart watches, phone apps, and GPS tools. While social media companies like Facebook usually require that users agree with end-user licence agreements (EULA) which forfeit rights to their data, these broad agreements do not amount to the level of informed consent that may be warranted of a medical research community. Even in cases where such EULAs satisfied legal requirements for biomedical research purposes, they may not have achieved a stronger ethical requirement if the agreements fail to provide adequate information to research participants on what might be done with their data. These are key difficulties that are inherent in big data research but which were rarely observed in traditional research methods. Furthermore, given the sheer volume and fast pace of big data and AI-facilitated biomedical research, it is important to consider the limits of consent and instead whether more robust governance frameworks can and should provide the necessary protections for research participants' data and wider interests. Such mechanisms should be charged with striking the delicate acceptable balance between safeguarding data confidentiality and preventing misuse, while not unduly stifling or impeding the progress of innovation and technology.

d. Extent of data security obligations vs value of data – The value of datasets is determined not only by its utility in research, but also the harms that might occur if such personal data is misused or lost. The value of such data should be determined by an independent data protection officer who would assign the appropriate data classification. This in turn determines the security requirements for handling, processing, storage and access to the data. Because it is difficult and unethical for data collectors to determine the sensitivity of the data, they should follow institutional guidelines for labelling data. As the costs of implementing data security measures are significant, the extent to

[26] Decentralised data refers to data generated from multiple sources or decentralised platforms such as digital health mobile applications or a combined data repository.

which unimportant or lowly-valued data (from the perspective of the data subject) requires dedicated protection may have to be proportionately considered. Additionally, they should reclassify the data sensitivity if they are merged with other datasets, or additional correlations added. When robust and proportionate mechanisms for data security are in place, lower-risk endeavours can be accommodated.

e. Different ethics understanding by non-biomedical third parties – As AI is often developed by third parties (e.g., developers, designers, engineers) who are unlikely to be part of the biomedical research or clinical sectors, they may have a different understanding of ethical concerns due to their distinct training, sensitivities, inclinations, and priorities. Proactive education and on-going engagement are needed to bridge such gaps because a failure to do so may not only compromise big data initiatives but also have trickle downstream effects to cause wider issues in the future.

Objective and Scope of Advisory Report

3.13 Due to the ethical issues and considerations on the use of big data and AI in biomedical research, the Bioethics Advisory Committee (BAC) has conducted a review and developed this advisory report to guide academics, healthcare professionals, researchers and Institutional Review Boards (IRBs) on the ethical principles of big data and AI use in biomedical research.

3.14 The main scope of the advisory report will focus on discussing ethical issues arising from the use of big data and AI in **biomedical research** such as responsible data usage, data ownership, custodianship, and stewardship, data privacy, accessibility and security, data anonymisation and other ethical considerations and issues specific to AI. The approach is to identify ethical principles to guide such use, namely, respect for persons, solidarity, justice, proportionality, sustainability and other ethical considerations (integrity, transparency, accountability, consistency and stakeholder engagement). This report builds upon previous BAC reports and recommendations to avoid potential misalignments, and reference relevant legislations/ Acts such as the Personal Data Protection Act (2012)[27] and the Human Biomedical Research Act (2015).[28]

3.15 This advisory report is intended to complement other big data and AI reports and ethical guidelines such as the Ethics Framework for Big Data in Health and Research by the Science, Health, and Policy-relevant Ethics in Singapore (SHAPES) working group[29] and the AI in Healthcare Guidelines co-developed by the Ministry of Health (MOH), the Health Sciences Authority (HSA), and the Integrated Health Information Systems (IHiS),[30] aimed to provide ethical guidance to decision-makers

[27] Personal Data Protection Act 2012 (2020 Revised Edition). *Singapore Statutes Online*. https://sso.agc.gov.sg/Act/PDPA2012

[28] Human Biomedical Research Act 2015 (2020 Revised Edition). *Singapore Statutes Online*. https://sso.agc.gov.sg/Act/HBRA2015

[29] Xafis, V., Schaefer, G. O., Labude, M. K. *et al.* (2019). An Ethics Framework for Big Data in Health and Research. *Asian Bioethics Review, 11*(3), 227–254. https://doi.org/10.1007/s41649-019-00099-x

[30] AI in Healthcare Guidelines. (2022). *Ministry of Health.* Retrieved December 13, 2022. https://www.moh.gov.sg/licensing-and-regulation/artificial-intelligence-in-healthcare

who work with big data in health and research, and improve the understanding, codify good practice and support the safe growth of AI in biomedical and healthcare research respectively.

CHAPTER 4: THE PROMISE OF BIG DATA AND AI RESEARCH STUDIES: APPLICATIONS, BENEFITS, AND RISKS

This chapter discusses the nature of big data and the applications of big data and AI use in biomedical research, challenges, as well as the corresponding benefits, risks, and ethical considerations.

The Nature of Big Data

4.1 With advances in technology, the use of big data and AI in biomedical research has become increasingly important, to enable researchers and healthcare professionals to combine and analyse massive datasets, identify patterns or correlations, generate useful insights and make faster and better data-driven decisions. These applications include the monitoring of diseases and outbreaks, predicting of health behaviours and disease outcomes, and providing risk stratification for individual patients and facilitate care management. While the growing use of big data and AI use in biomedical research promises several benefits, there are challenges and risks that come with the use of AI and machine learning processes, predictive modelling and other advanced analytics applications, and technologies. This chapter discusses the nature of big data and explains how big data and AI are used in biomedical research, their applications, challenges, and benefits and risks and their value to biomedical research.[1]

4.2 Big data is a collection of both structured and unstructured data that is huge in volume and rapidly generated. The amount of big data produced grows exponentially with time, and the amount is expected to double every two years. Such tremendously large data sets cannot be analysed by humans alone and require computational analysis to reveal new trends or associations.[2] The use of big data also comes with different concerns such as capturing, integrating, transforming, analysing, and interpreting big data; and the need to address privacy concerns, data security, governance, and data sharing, as well as operational and ownership issues.[3] Big data can be characterised by the 3Vs: volume, variety, and velocity[3, 4, 5], and the corresponding key challenges in its use are as follows:

a. Volume refers to the sheer quantity of data, taking into account the number of persons whose data is contained in given datasets and the level of detail about each individual. This results in large volumes of data that can be analysed or stored. The management of this large volume of data coupled with the heterogeneity, ubiquity and dynamic nature of data generated from varying

[1] Floridi, L. (2012). Big Data and Their Epistemological Challenge. *Philosophy & Technology, 25*(4), 435–437. https://doi.org/10.1007/s13347-012-0093-4

[2] Emanuel, E. J., & Wachter, R. M. (2019). Artificial Intelligence in Health Care. *JAMA*, *321*(23), 2281. https://doi.org/10.1001/jama.2019.4914

[3] Sivarajah, U., Kamal, M. M., Irani, Z. *et al*. (2017). Critical Analysis of Big Data Challenges and Analytical Methods. *Journal of Business Research*, *70*, 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001

[4] Baro, E., Degoul, S., Beuscart, R. *et al*. (2015). Toward a Literature-driven Definition of Big Data in Healthcare. *BioMed Research International, 2015,* 1–9. https://doi.org/10.1155/2015/639021

[5] Xafis, V., Schaefer, G.O., Labude, M.K. *et al*. (2019). An Ethics Framework for Big Data in Health and Research. *Asian Bioethics Review, 11*(3), 227–254. https://doi.org/10.1007/s41649-019-00099-x

programmes and devices, makes determining, retrieving, processing, integrating, and inferring of data a difficult task.[6]

b. Variety refers to the substantial diversity of data forms about individuals; data may be structured, or unstructured and can come from a diversity of sources (e.g., scientific data, user-generated data, and web data). The data may not be consistent and not follow a specific template or format (e.g., messages as text, email, tweets, blogs; transactional data as web logs, business transactions, scientific data from data-intensive experiments giving genome and healthcare data).[7, 8] Such heterogeneity poses a challenge to the comprehension and management of data.[9]

c. Velocity refers to the great and increasing speed at which data can be transmitted and analysed. There is difficulty in managing the rapid and increasing generation of non-homogenous data, which is either from the creation of new data or updating of existing data.[6] Such processing is especially important if time-sensitive, geospatial-sensitive data needs to be sorted quickly for real-time analytics.

4.3 Pertinent to BAC's review in this area, data process issues (capturing, integrating, transforming, analysing, and interpreting big data), management challenges (privacy concerns, data security, governance and data sharing), as well as other operational and ownership issues associated with the use of big data and AI in biomedical research are of interest. Some challenges are listed as follows:

Data process challenges

a. Collecting and storing of data: Lack of data lineage and discrepancies of scale[10, 11] may further hamper the rate by which data is captured and stored. This in turn reduces the effectiveness in extracting actionable material from the data.[12]

b. Extracting, cleaning, aggregating and integrating data: These tasks can become difficult as big data is highly varied and inter-connected.[6] Healthcare data in particular is messy, missing and heterogenous.[13]

[6] Zhao, Z., Zhang, R., Cox, J. *et al*. (2013). Massively Parallel Feature Selection: An Approach Based on Variance Preservation. *Machine Learning 92*, 195–220. https://doi.org/10.1007/s10994-013-5373-4

[7] Chen, J., Chen, Y., Du, X. *et al*. (2013). Big Data Challenge: A Data Management Perspective. *Frontiers of Computer Science, 7*, 157–164. https://doi.org/10.1007/s11704-013-3903-7

[8] Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly, 36(*4), 1165. https://doi.org/10.2307/41703503

[9] Labrinidis, A., & Jagadish, H. V. (2012). Challenges and Opportunities with Big Data. *Proceedings of the VLDB Endowment*, *5*(12), 2032–2033. https://doi.org/10.14778/2367502.2367572

[10] Wang, Y., & Wiebe, V. J. (2016). Big Data Analytics on the Characteristic Equilibrium of Collective Opinions in Social Networks. *Big Data*, 1403–1420. https://doi.org/10.4018/978-1-4666-9840-6.ch064

[11] Paris, J., Donnal, J. S., & Leeb, S. B. (2014). NilmDB: The Non-Intrusive Load Monitor Database. *IEEE Transactions on Smart Grid, 5*(5), 2459–2467. https://doi.org/10.1109/TSG.2014.2321582

[12] Chen, P. C. L., & Zhang, C.Y. (2014). Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data. *Information Sciences, 275,* 314–347. https://doi.org/10.1016/j.ins.2014.01.015

[13] Ngiam, K.Y., & Khor, I.W. (2019). Big Data and Machine-Learning Algorithms for Healthcare Delivery. *The Lancet Oncology, 20*(5), E262–E273. https://doi.org/10.1016/S1470-2045(19)30149-4

c. Analysing, interpreting and modelling of data: Data analysis used to rely on the relationships between data collected from collaboration networks. However, as unrelated databases become more common, past methods for data analysis, interpretation and modelling are no longer applicable as a result of today's need for exceptional capacity and computing power.[14]

Data management challenges

a. Privacy: Privacy becomes a particularly acute concern when collection and analysis of big data, and real-time location-based services are being conducted over the internet and transmitted over networks.[15] Risks to privacy can be heightened in myriad ways.

b. Security: The distributed nature of big data storage and processing makes it complex and potentially more vulnerable to attacks.[16]

c. Data governance: There may be additional challenges in data governance, particularly for unstructured big data as categorising, modelling and mapping data is less straightforward.[17] Governance regimes may extend across multiple sectors or ecosystems with different values and interests at stake.

Applications of Big Data and AI Use in Biomedical Research

4.4 Useful applications of big data and AI use in biomedical research include longitudinal and cross-sectional assessments (e.g., research on the effectiveness of specific medical interventions across hospitals),[18] longitudinal monitoring of chronic conditions and well-being (e.g., collection and analysis of data from cohorts of patients with chronic diseases over a long period of time via wearables and lightweight health devices)[19] and AI-driven simulation for biological models (e.g., computational modelling assistant, which constructs concrete simulations after researchers have inputted relevant hypotheses, methods and databases).[20] As mentioned in Chapter 3, 'Introduction', machine learning used in AI is also used for

[14] Edwards, R., & Fenwick, T. (2015). Digital Analytics in Professional Work and Learning. *Studies in Continuing Education, 38*(2), 213–227. https://doi.org/10.1080/0158037x.2015.1074894

[15] Yi, X., Liu, F., Liu, J. *et al*. (2014). Building a Network Highway for Big Data: Architecture and Challenges, *IEEE Network*, *28*(4), 5–13. https://doi.org/10.1109/MNET.2014.6863125

[16] Bertot, J. C., Gorham, U., Jaeger, P. T. *et al*. (2014). Big Data, Open Government and E-Government: Issues, Policies and Recommendations. *Information Polity, 19*(1–2), 5–16. https://doi.org/10.3233/ip-140328

[17] Lawton, G. (2020). 6 Best Practices on Data Governance for Big Data Environments. *TechTarget.* (2020, February 10). Retrieved December 9, 2022. https://www.techtarget.com/searchdatamanagement/tip/6-best-practices-on-data-governance-for-big-data-environments

[18] Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 239–273. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip

[19] Boye, N. (2012). Co-production of Health Enabled by Next Generation Personal Health Systems. *Studies in Health Technology Informatics, 177,* 52–58. PMID: 22942030

[20] Rong, G., Mendez, A., Assi, E.B. *et al*. (2020). Artificial Intelligence in Healthcare: Review and Prediction Case Studies. *Engineering, 6*(3), 291–301. https://doi.org/10.1016/j.eng.2019.08.015

drug development, and identifying patterns and relationships not captured by traditional statistical methods.[21]

4.5 The newest and probably the most significant source of big data used in biomedical research would be electronic health-related data collected via health platforms such as electronic health records, personal health monitoring technologies, home sensors, social media applications, healthcare related forums, patient portals, biomedical search queries on search engines and generic databases. A combination of different data sources presents new avenues for deeper insights to be generated.[22] These new data sources accompany traditional data repositories which include data from aggregated clinical trials, biological specimens, administrative hospital data and genome sequencing data.[23, 24]

4.6 In considering AI as an application of big data use in biomedical research, such AI systems are powered by algorithms such as machine learning and deep learning. There are various types of AI approaches involving humans. In this report, we focus on a type of AI called narrow AI that is more typical in practical applications, and define artificial general intelligence (AGI) as being outside of scope for biomedical research.

a. Narrow AI is an AI type that makes use of algorithms to exploit large-scale data via deep learning to make predictions, and has been successfully realised to date. It does not mimic or replicate human intelligence but is goal-oriented and designed to perform singular tasks.

b. AGI refers to a true intelligence that would be indistinguishable from human intelligence and can be applied to general problem solving, and present as a technology for broader or general purposes. Currently, AGI with general capabilities does not yet exist and there is no use of AGI in biomedical research.[25, 26]

4.7 AI approaches or the human-AI relationship may be understood as human-in-the-loop, human-out-of-the-loop, or human-in-command.

a. Human-in-the-loop models refer to systems which allow humans to give direct feedback to an AI model when the machine or computer system is unable to offer an answer to a problem, thus needing human intervention. Studies have

[21] Rodriguez, F., Scheinker, D., & Harrington, R. A. (2018). Promise and Perils of Big Data and Artificial Intelligence in Clinical Medicine and Biomedical Research. *Circulation Research*, *123*, 1282–1284. https://doi.org/10.1161/CIRCRESAHA.118.314119

[22] Lupton, D. (2014). The Commodification of Patient Opinion: The Digital Patient Experience Economy in the Age of Big Data. *Sociology of Health & Illness, 36*(6), 856–869. https://doi.org/10.1111/1467-9566.12109

[23] Costa, F. F. (2014). Big Data in Biomedicine. *Drug Discovery Today, 19*(4), 433–440. https://doi.org/10.1016/j.drudis.2013.10.012

[24] McGuire, A. L., Colgrove, J., Whitney, S. N. *et al.* (2008). Ethical, Legal, and Social Considerations in Conducting the Human Microbiome Project. *Genome Research, 18*(12), 1861–1864. https://doi.org/10.1101/gr.081653.108

[25] Floridi L (2018). The Ethics of Artificial Intelligence. In: Franklin, D. (Ed.), *Megatech: Technology in 2050*. (pp. 155–163). London: Profile Books.

[26] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep Learning. *Nature, 521*, 436–444. https://doi.org/10.1038/nature14539

shown that such an approach also provides an important safety mechanism for detecting and correcting algorithmic errors that may occur.[27, 28] An example of a human-in-the-loop model is the use of automated image AI tools in radiology e.g., X-ray, CT scans, ultrasound, and MRI images to detect deformities and tumours. AI algorithms can automatically detect complex anomalous patterns in image data to provide an assistive diagnosis for patients.[29]

b. Human-out-of-the-loop models are focused on removing human interventions and allowing the machine or algorithm to perform learning and decision-making on its own (e.g., in autonomous driving). This may be a suitable model when there is a need to remove human biases during the decision-making process while retaining human oversight of analysis outputs and is often recommended for situations that require quality control features.[30]

c. Human-in-command models refer to AI systems where humans always retain control over the machine, combining individual human knowledge with the potential of machine-learning systems that function as tools to enhance human capabilities. The human determines which tasks are delegated to AI and which decisions the AI is allowed to make.[31] An instance of the human-in-command approach is when an electrocardiogram (ECG) machine, which is activated by humans, performs a test and generates an ECG trace which is analysed by humans to determine heart problems and detect common heart conditions.[32]

4.8 In terms of categorising big data and AI in biomedical research, for the purpose of this report, we will focus on examining (a) cohort studies using/involving big data and (b) studies using/involving real-world big data, where both types of studies can involve data collected prospectively or retrospectively.

a. In cohort studies, data is collected in an experimental, interventional, controlled or randomised controlled trial (RCT) setting where data is collected based on variables that are controlled or monitored. Examples include clinical trials investigating the safety and efficacy of investigational products (e.g., pharmaceutical substances like cancer drugs, or HIV antiretroviral drugs being tested or used as a reference in a clinical trial).[33]

[27] Kumar, V., Smith-Renner, A., Findlater, L. *et al*. (2019). Why Didn’t You Listen to Me? Comparing User Control of Human-In-The-Loop Topic Models. *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*. https://doi.org/10.18653/v1/p19-1637

[28] Wu, X., Xiao, L., Sun, Y. *et al*. (2022). A Survey of Human-In-The-Loop for Machine Learning. *Future Generation Computer Systems, 135*, 364–381. https://doi.org/10.1016/j.future.2022.05.014

[29] Ghayvat, H., Awais, M., Bashir, A.K. *et al*. (2022). AI-enabled Radiologist in the Loop: Novel AI-based Framework to Augment Radiologist Performance for COVID-19 Chest CT Medical Image Annotation and Classification from Pneumonia. *Neural Computing and Applications: Special Issue on Machine Learning for Big Data Analytics in Smart Healthcare Systems*. 1–19. https://doi.org/10.1007/s00521-022-07055-1

[30] Abbass, H. A. (2019). Social Integration of Artificial Intelligence: Functions, Automation Allocation Logic and Human-Autonomy Trust. *Cognitive Computation, 11*, 159–171. https://doi.org/10.1007/s12559-018-9619-0

[31] Holmberg, L. (2021). Human-In-Command Machine Learning. *Studies in Computer Science - Malmö: Malmö Universitet, 16*, 136. https://doi.org/10.24834/isbn.9789178771875

[32] Gade, A., & Maddi, R. (2022). Artificial Intelligence-based Software as Medical Device. *World Journal of Current Medical and Pharmaceutical Research, 4*(3), 29–32. https://doi.org/10.37022/wjcmpr.v4i3.212.

[33] Chodankar, D. (2021). Introduction to Real-World Evidence Studies. *Perspectives in Clinical Research, 12*(3), 171–174. https://doi.org/10.4103/picr.picr_62_21

b. Real world data is data that is not collected under experimental, or interventional, or controlled conditions i.e., data not collected in the context of a RCT, but data generated in routine care or clinical practice, or data generated from the delivery of healthcare in non-controlled settings. Examples include electronic health records (EHRs), medical claims, billing data, and insurance data, data from product and disease registries, patient-generated data, including from in-home-use settings, data gathered from other sources that can inform on health status, such as mobile devices (measuring individual or environmental parameters).[33]

Benefits, Risks and Other Ethical Considerations of Big Data and AI Use in Biomedical Research

4.9 The ability of big data and AI to aggregate, integrate and process massive amounts of data from various sources has yielded benefits such as (i) better prediction and diagnostic tools; (ii) improvements in quality and effectiveness of clinical services; and (iii) advancements in personalised medicine. With the help of data analytics tools, it has become more accessible for researchers to integrate knowledge and expertise across multiple disciplines such as biology, computer science, mathematics, statistics, and physics to find practical clinical solutions in areas such as cardiac diseases[34], cardiometabolic health adversities[35], cancer research[36], and drug discovery.[37]

4.10 Some notable examples that demonstrate how big data and AI, when used appropriately, can reap immense benefits such as gaining meaningful clinical and patient insights from databases to inform diagnoses and clinical management decisions include:

a. US – National Institutes of Health 1000 Genomes Project, the world’s largest human genetic variation dataset, is a database of genomic data that is well referenced for studying genetic basis of diseases. The data, cell lines and DNA samples from the associated Coriell Institute are fully accessible to all researchers and the public.[38]

b. UK – Moorfields Eye Hospital NHS Foundation Trust partnership with DeepMind applied machine learning to one million anonymous eye scans to look for early signs of eye conditions such as age-related macular degeneration

[34] Madani, A., Arnaout, R., Mofrad, M. *et al*. (2018). Fast and Accurate View Classification of Echocardiograms Using Deep Learning. *Npj Digital Medicine, 1*(1). https://doi.org/10.1038/s41746-017-0013-1

[35] Landry, M. D., van Wijchen, J., Hellinckx, P. *et al*. (2022). Artificial Intelligence and Data-Driven Rehabilitation: The Next Frontier in the Management of Cardiometabolic Disorders. *Archives of Physical Medicine and Rehabilitation, 103*(8), 1693–1695. https://doi.org/10.1016/j.apmr.2022.03.022

[36] Jiang, P., Sinha, S., Aldape, K. *et al*. (2022). Big Data in Basic and Translational Cancer Research. *Nature Reviews Cancer*, *22*(11), 625–639. https://doi.org/10.1038/s41568-022-00502-0

[37] Zhu, H. (2020). Big Data and Artificial Intelligence Modeling for Drug Discovery. *Annual Review of Pharmacology and Toxicology, 60*(1), 573–589. https://doi.org/10.1146/annurev-pharmtox-010919-023324

[38] IGSR: The International Genome Sample Resource. (2022). *1000 Genomes Project Summary.* Retrieved December 9, 2022. http://www.internationalgenome.org/1000-genomes-summary

and diabetic retinopathy that can be prevented by early detection and treatment.[39]

c. Imaging informatics comprising methods for generating, managing and representing medical imaging data is being continuously transformed with the use of big data and AI for imaging data to be incorporated into EHRs to provide deeper insights.[40]

4.11 The use of big data and AI tools has shifted researchers' experience from a single medical/clinical activity perspective to a population view comprising an integrated view of big data and health, especially so with the ability to include geographical and environmental information. This further increases the ability to interpret gathered data and extract new knowledge, and is especially important for research advancements in infectious diseases surveillance and the understanding of population health.[41]

4.12 While huge potential exists to advance biomedical research using big data and AI, there could be complex and multi-dimensional challenges arising from advances in big data and AI technologies and their application in biomedical research. Though many of the ethical issues surrounding biomedical research concerning big data and AI are not drastically different from that of the current research landscape, the innate sensitivity of health-related data and the implicit vulnerability of individuals or patients carries greater ethical weight which should be recognised. Some concerns include issues with consent, data governance and responsible data use.

a. Given the sensitivity of personal medical data and the changing climate of data collection and use, consent models may need to be revisited in the context of big data and AI use in biomedical research. Traditional consent models may be infeasible or impracticable where data is collected from multiple sources or used for multiple purposes (i.e., secondary and tertiary data uses). Consent models may be different for traditional and non-traditional sources of data, where traditional sources of data comprise medical or research data for which explicit, informed consent is typically taken upfront, whilst explicit, informed consent for non-traditional sources of data (e.g., consumer data, social media data, data from wearables and sensors) is not common.

b. Different from the usually obvious direct discrimination by humans, the development of AI algorithms or models carries the risks of obscurely biased AI algorithms and models. The responsibility and accountability of researchers in ensuring that data fed into the algorithm is not biased or results in bias-driven outcomes is therefore a key mitigating factor. The need for robust assessment of fairness of outcomes is crucial as inadequate representation leading to inherent biases in datasets may result in inaccurate/skewed

[39] Moorfields Eye Hospital NHS Foundation Trust (2022). DeepMind Health Q&A. *Moorfields Eye Hospital NHS Foundation Trust.* Retrieved December 9, 2022. https://www.moorfields.nhs.uk/faq/deepmind-health-qa

[40] Luo, J., Wu, M., Gopukumar, D. *et al*. (2016). Big Data Application in Biomedical Research and Health Care: A Literature Review. *Biomedical Informatics Insights, 8*. https://doi.org/10.4137/bii.s31559

[41] Hay, S. I., George, D. B., Moyes, C. L. *et al*. (2013). Big Data Opportunities for Global Infectious Disease Surveillance. *PLoS Medicine, 10*(4). https://doi.org/10.1371/journal.pmed.1001413

conclusions and mechanisms to ensure accountability and responsibility for AI systems and their outcomes should be carefully assessed and put in place.

c. Responsible data use reduces discrimination risks arising from biases or data re-identification as well as ensure appropriate processes are in place to manage incidental findings. There are risks of discrimination arising from participation in research or biases from biomedical research (e.g., individuals who participated in genetic research and their eligibility for insurance; or certain ethnic groups have been shown to have genetic predisposition to certain diseases). Increasing use of big data and AI in biomedical research also increases the return of incidental findings which may make management and communication of such findings to research participants more complex and challenging. Researchers should inform research participants on the possibility of incidental findings arising from the research and seek their consent on the return of such findings during the consent taking process, prior to the commencement of the research.

4.13 Given the issues that need to be re-examined, the subsequent chapters will discuss in detail the ethical principles (Chapter 5) and considerations of fair data usage (Chapter 6), data custodianship (Chapter 7), data privacy, security and accessibility (Chapter 8), anonymisation, and the de-and-re-identification of data (Chapter 9), consent (Chapter 10), responsibility to public in data-sharing (Chapter 11), legacy data (Chapter 12), AI-specific issues (Chapter 13) and BAC’s recommendations (Chapter 14) to guide academics, researchers, healthcare professionals and IRBs on the ethical use of big data and AI in biomedical research.

CHAPTER 5:GENERAL ETHICAL PRINCIPLES TO GUIDE BIG DATA AND AI BIOMEDICAL RESEARCH DEVELOPMENTS IN SINGAPORE

This chapter provides an overview and discusses the general ethical principles to guide big data and AI use in biomedical research in Singapore.

General Ethical Principles

5.1 In relation to the use of big data and AI in biomedical research, the BAC stays guided by both substantive[1] and procedural principles. Substantive principles[2] include considering *'Respect for persons'*, *'Solidarity'*, *'Justice'*, *'Proportionality'* and *'Sustainability'*, which are discussed in greater detail as follows:

a. Respect for persons

5.2 *Respect for persons* includes respecting their right to make decisions without being coerced, misled, or kept in ignorance. The BAC refers to this as autonomy which can be broadly defined as the right of individuals to decide and act on their own volition and according to their own assessment of their interests. The welfare and interests of individuals are to be protected, especially when their autonomy is impaired or lacking. This principle underlies the importance that is often given to informed or appropriate consent to participate in research, protection of privacy, safeguarding confidentiality, and avoiding or minimising harm to research participants. The principle of respect for autonomy also includes proper regard for religious and cultural diversity in understanding of what constitutes the good or good life.

5.3 The principle of *respect for persons* or autonomy in big data and AI use in biomedical research can be demonstrated in the moral stance or attitude towards individuals (or groups). One of the ways this principle can be conveyed is through adequate communication.[3] An individual's autonomy can be compromised when they are unaware of the nature and aims of the research they participate in and the unexpected information that may be generated from the use of their data in research (e.g., incidental findings). In a paradigm biomedical research consent such as involvement in clinical trials, informed consent is often the gatekeeper ethical tool that is used. Typically, this requires that research participants are fully informed and have a reasonably comprehensive understanding of the nature and purpose of data collection, the methodology used, the potential risks and benefits of participation in the research, and possible future uses of the research involving AI and data being conducted. The participants should also be informed that they may withdraw from the research at any time without having to provide any explanation or justification, and without penalty or prejudice to any treatment they may be receiving (see more discussion in Chapter 10: Revisiting Consent in the Arena of Big Data and AI).

[1] Substantive principles are considerations that should be realised through the outcome of a decision.

[2] Bioethics Advisory Committee. (2022). Ethical Principles. *Bioethics Advisory Committee*. Retrieved November 23, 2022. https://www.bioethics-singapore.gov.sg/who-we-are/ethical-principles/

[3] Xafis, V., Schaefer, G. O., Labude, M. K. *et al*. (2019). An Ethics Framework for Big Data in Health and Research. *Asian Bioethics Review*, *11*(3), 227–254. https://doi.org/10.1007/s41649-019-00099-x

5.4 Given the rapid pace of evolution in AI technology, in some instances, researchers may need to obtain periodic re-consent from participants, instead of relying on a one-time consent, to update them on new information and facilitate better awareness of emerging uses, as part of ongoing informed consent process. Such consent taking process safeguards individuals' autonomy and enables individuals to make informed autonomous decisions on whether to participate in the research and the use of their personal data.[4]

b. Solidarity

5.5 The BAC asserts that as some degree of mutual obligation exists between the individual and society, common interests of society may constrain individuals' autonomy and interests in specified circumstances. The principle of *solidarity* reflects the willingness and moral obligations of individuals to share the costs associated with research participation, such as potential risks, in return for the common good. *Solidarity* thus reflects the importance of altruism and other prosocial motivations and justifications as a basis for participation in biomedical research. There is a need to balance the interests of the public or society with the rights and interests of individual participants. Conflicting and irreconcilable ethical perspectives should be resolved by balancing public and individual interests. Based on the principle of *solidarity*, the BAC acknowledges that public interest may override individual rights and interests in certain circumstances, such as in public health and epidemiological research; and where appropriate safeguards are in place and the research poses minimal risk, requirements for obtaining informed consent or appropriate consent may be subordinated to those of public interests.

5.6 In the context of big data and AI use in biomedical research, data protection has been a key tenet of the governance model focused on privacy and individual rights. Such a governance model has been criticised for its focus on individual rights and interests, at the cost of collective and group interests.[5] A *solidarity*-based data governance model may need to be considered to address this issue to promote sound biomedical research and to foster equitable and collective sharing in the benefits and costs of digital practices, while also appropriately respecting individual autonomy.[5]

c. Justice

5.7 The principle of *justice* in the context of biomedical research encompasses the general principles of fairness and equity, which imply that access to the benefits of research, and the burden of supporting it, should be equitably and fairly shared in society. In the event that research yields an immediate benefit that could apply to participants in the research, reciprocity as a sub-set/element of the principle of *justice* would dictate that the benefits be offered to them. The principle of *justice* also implies that researchers and their institutions shoulder some responsibility for the welfare of participants in the event of adverse outcomes arising directly from their participation in the research.

[4] Howe Iii, E. G., & Elenberg, F. (2020). Ethical Challenges Posed by Big Data. *Innovations in Clinical Neuroscience, 17*(10–12), 24–30. https://pubmed.ncbi.nlm.nih.gov/33898098/

[5] Prainsack, B., & Buyx, A. (2013). A Solidarity-based Approach to the Governance of Research Biobanks. *Medical Law Review*, *21*(1), 71–91. https://doi.org/10.1093/medlaw/fws040

5.8 *Justice* in the context of big data and AI biomedical research requires that researchers manage and use data in a manner that does not create or reinforce bias. Algorithms that have been trained using data obtained from biased systems (e.g., data predominantly obtained from a single group based on race, ethnicity, country of origin, or socioeconomic class) are likely to produce biased results, leading to decisional bias or skewed conclusions.[4] These conclusions may perpetuate injustice as they tend to primarily benefit the overrepresented group while the same benefits may not translate to the underrepresented groups,[6] and may even possibly harm these populations. For example, a particular treatment that benefits one group of people may cause adverse side effects in another. Effective safeguards should be available against biased algorithmic determination and any associated discrimination.[7] Institutions or committees approving data access should enforce the principle of *justice* by providing recommendations for data collation or evaluation procedures to reduce bias (on specific case-by-case basis) prior to approval and access provision. Nonetheless, in some instances, data obtained from biased systems may not necessarily be inaccurate but could be attributed to the algorithm rather than the data itself. The data may still accurately show that a minority racial group is disproportionately represented in criminal behaviour or have a higher incidence of chronic medical conditions due to other socio-economic and cultural reasons, and such data should not be used to perpetuate or reinforce biased decisions against that group.

d. Proportionality

5.9 The principle of *proportionality* requires that the methods or processes used in biomedical research are necessary and appropriate in relation to the research intent and the range of public and private interests at stake.[3] Regulation of biomedical research should be proportional to the degree of possible threats to individual freedom, welfare, or the public good. As such, interference with individuals' autonomy, including their decisions, actions, or rights in carrying out or participating in research, should not exceed what is needed to achieve regulatory aims of mitigating anticipated threats and risks, and in promoting public interest. The risks in biomedical research and stringency of its regulation are acceptable if they are proportionate to potential benefits to the participant or others (e.g., future patients).

5.10 When assessing the processing of personal data for big data and AI use in biomedical research, *proportionality* requires that only personal data which is adequate for data robustness and quality and is relevant for the purposes of data processing is collected and used. Equally, the right to protection of personal data, while important, may not be the singular or primary objective in all situations and must be considered in relation to the common good, and be balanced against other fundamental rights, and executed in accordance with the principle of *proportionality*.[8] Thus, for adequately anonymised or securely de-identified data, a 'light touch' or moderate regulation may be most appropriate in balancing individual rights with public interests. This

[6] Wang, F., Casalino, L. P., & Khullar, D. (2019). Deep Learning in Medicine-Promise, Progress, and Challenges. *JAMA Internal Medicine, 179*(3), 293–294. https://doi.org/10.1001/jamainternmed.2018.7117

[7] UNESCO (2022). *Recommendation on the Ethics of Artificial Intelligence.* Retrieved November 23, 2022. https://unesdoc.unesco.org/ark:/48223/pf0000381137

[8] General Data Protection Regulation (Recital 4) (2016). *Official Journal of the European Union.* (2016, May 4). Retrieved November 23, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

entails that there should be safeguards in place to mitigate the risk of re-identification while allowing uses of the data for sound scientific research (see more discussion in Chapter 9: Anonymisation, De- and Re-identification of Data).

e. Sustainability

5.11 The principle of *sustainability* can be understood broadly to support arguments for the fair and just conservation of nature and minimisation of resource depletion for the good of the planet. Thus, research processes and outcomes should not unfairly jeopardise or prejudice the welfare of future generations.

5.12 The advent of big data and AI technologies can either benefit *sustainability* objectives or hinder their realisation, depending on their applications. Researchers have a complementary responsibility to reduce the environmental impact of big data and AI systems, including but not limited to their carbon footprint and energy consumption, to minimise climate change and environmental risk factors, and avoid the unsustainable exploitation, use and transformation of natural resources contributing to the deterioration of the environment and the degradation of ecosystems.[7, 9]

5.13 Given their synergistic relationship, big data and AI, when used in tandem, can be harnessed to provide effective solutions to address environmental challenges and issues, and achieve sustainable development. Big data techniques allow for effective handling, processing and analysis of environmental data that may be complex in terms of volume, heterogeneity, and velocity. Integrating machine learning with big data can deepen the understanding of patterns from environmental data and allow meaningful insights to be drawn from the data.[10]

5.14 In addition to the substantive principles, the BAC has identified three procedural principles[11] as being particularly important in the context of using big data and AI in biomedical research. These principles are intended to guide individual researchers and IRBs in ethical decision-making and may assist in realising the BAC's guiding principles *(respect for persons, solidarity, justice, proportionality, sustainability)* and determining the appropriate method or process to be used when collecting, receiving, using, storing, sharing, transferring, and processing research participants' data.

I. Integrity, transparency, and accountability

5.15 Researchers and their institutions should uphold the highest possible standards of professional and moral conduct during the conduct of biomedical research (principle

[9] Samuel, G., & Richie, C. (2022). Reimagining Research Ethics to Include Environmental Sustainability: A Principled Approach, Including a Case Study of Data-Driven Health Research. *Journal of Medical Ethics.* https://doi.org/10.1136/jme-2022-108489

[10] Sustainability – Sustainable Engineering and Science. (2022). Special Issue: Applications of Machine Learning and Big Data Analytics for Environmental Sustainability. *MDPI.* Retrieved November 23, 2022. https://www.mdpi.com/journal/*Sustainability*/special_issues/big_data_enviro_sus

[11] Procedural principles guide the process of deliberation and decision-making itself. Procedural principles may assist in realising certain substantive principles (e.g., transparency (procedural) can help promote *justice* (substantive) by allowing scrutiny from third parties who may be able to point out potential research discrepancies) and determining which substantive values to prioritise.

of *integrity*), and should open their decision-making considerations, processes, and actions to public scrutiny (principle of *transparency*). The level of transparency should always be calibrated to the context and impact, as there may be a need to balance transparency with other principles such as data protection, safety, and security. For example, there may be circumstances where individuals are not aware of how their data is being accessed or used. Nonetheless, they should be fully apprised when a decision is informed by or made based on AI algorithms, especially when it affects their safety, interests or rights, and they should be able to access the reasons, including ethical reasons, for such decisions.[7] *Transparency* relates closely to the principle of *responsibility* and *accountability*. Ethical responsibility and liability for the decisions and actions arising directly from research studies should be attributed to researchers and their institutions.

II. Consistency

5.16 The principle of *consistency* dictates that the same ethical standards should be applied across similar situations to ensure fairness and trustworthiness. In this regard, IRBs and equivalent bodies should adhere to a practice of consistency. This includes using the same or similar required standards to evaluate research applications and protocols for research studies involving the use of big data and AI to protect the welfare, rights, and privacy of human subjects participating in these studies. IRBs should adhere to standards set out in advisories or guidelines issued by national advisory bodies, i.e., BAC’s 2021 Ethics Guidelines.

III. Stakeholder engagement

5.17 Stakeholder engagement extends beyond dissemination of information and further requires that decision-makers consider the views of all stakeholders, and take these into account where possible. Researchers and institutions should first define the stakeholders to be engaged and the processes for such engagements, particularly if they are considering access to significant data resources. Researchers and institutions who intend to use big data in biomedical research should consult relevant stakeholders such as research participants to explain the purpose of data usage and the parties who would be accessing their data. Similarly, for the design and development of AI algorithms and models, researchers and institutions should engage key stakeholders such as users, developers, and the public to understand the views, feedback, and concerns of the various groups. Meaningful stakeholder engagement happens when there is an opportunity to influence what happens in the future. In the biomedical research context, this might be input to research design, ethical oversight or overall governance of the research and the research findings.

Relevant Data Governance Frameworks

5.18 While there is no specific legislation that governs the use of big data and AI in Singapore, there are established data governance frameworks that incorporate the aforementioned principles. These frameworks collectively address some of the ethical issues such as the possible role for consent and the imperative to have adequate protection of personal data arising from big data and AI use in biomedical research. All relevant data governance frameworks should be reviewed to keep up with the developments in big data and AI use in biomedical research in Singapore.

5.19 In 2014, the Personal Data Protection Act (PDPA) 2012[12] came into full effect to provide a baseline standard of protection for personal data[13] in Singapore. This Act complements sector-specific legislative and regulatory frameworks such as the Banking Act and Insurance Act. The Act sets out broad requirements governing the collection, use, disclosure, and care of personal data.[14] Under this Act, organisations may collect, use and/or disclose only the personal data of individuals who have provided consent and for the purpose(s) for which consent has been given by these individuals. Organisations should also implement security measures to protect the personal data in its possession or control to prevent any unauthorised access, collection, use and/or disclosure of such data. The PDPA 2012 also sets out exceptions with safeguards for collection, use and disclosure of personal data without consent for research purposes under the Second Schedule[15] (i.e., personal data is used in an individually-identifiable form; there is clear public benefit to using the personal data for research purpose; when it is impracticable for the research institution to seek the individual's consent for data disclosure; the results of the research will not be used to make any decision that affects the individual; and if the results of the research are published, the published results should not identify the individual).

5.20 In recognition that research should always be conducted with integrity and be of reliable quality to ensure that the health, welfare, and safety of research participants remain a paramount consideration, the Human Biomedical Research Act (HBRA) was enacted in 2015.[16] The HBRA provides clarity on the roles and responsibilities of individuals and entities involved in human biomedical research and the handling of human tissue in research. This Act includes requirements of appropriate consent for conduct of HBR and handling of human tissue in research, including cases of minors or vulnerable populations, and situations warranting waiver of consent. In addition, HBRA sets out safeguards for the collection, storage, use and disclosure of individually-identifiable health information where appropriate consent must be obtained from the research participant before the research can be conducted. The governance of de-identified data is covered under the Health Information Bill (not enacted at this juncture) and will not be discussed in this report.

5.21 To support patient safety and improve trust in the use of AI in healthcare, the Ministry of Health, Singapore co-developed the AI in Healthcare Guidelines 2021(AIHGIe)[17] with the Health Sciences Authority (HSA) and the Integrated Health Information Systems (IHiS). AIHGLe shares good practices with AI

[12] Personal Data Protection Act 2012 (2020 Revised Edition). *Singapore Statues Online*. https://sso.agc.gov.sg/Act/PDPA2012

[13] Under the PDPA, personal data is defined as data about an individual who can be identified from that data, or from that data and other information to which the organisation has or likely to have access.

[14] Personal Data Protection Commission. (2022). PDPA Overview. *Personal Data Protection Commission.* Retrieved November 23, 2022. https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[15] Personal Data Protection Act 2012 (2020 Revised Edition), Second Schedule, 'Additional Bases for Collection, Use and Disclosure of Personal Data without Consent', Part 3: 'Disclosure of Personal Data without Consent', Division 2: 'Research'. *Singapore Statutes Online.* https://sso.agc.gov.sg/Act/PDPA2012

[16] Human Biomedical Research Act 2015 (2020 Revised Edition). *Singapore Statues Online*. https://sso.agc.gov.sg/Act/HBRA2015

[17] AI in Healthcare Guidelines (2022). *Ministry of Health.* Retrieved November 23, 2022. https://www.moh.gov.sg/licensing-and-regulation/artificial-intelligence-in-healthcare

developers (e.g., AI medical device manufacturers or companies) and AI implementers (e.g., healthcare institutions such as hospitals, clinics, laboratories) to support patient safety and improve trust in the use of AI in healthcare. AI developers and implementors are encouraged to review the recommendations and make changes, where necessary, to their internal development and implementation governance and controls to align with these Guidelines. These include measures to prevent or minimise discriminatory or unjust clinical impact on patients across different demographic lines such as race or gender (e.g., ensuring testing datasets are representative) and introducing/enhancing safeguards to protect patients' interests, including their safety and well-being (e.g., establish processes to investigate any adverse events, and implement regular reviews for safety).

5.22 While the aforementioned data governance frameworks, to a very large extent, incorporate various ethical principles being discussed, and collectively address some of the ethical issues applicable to big data and AI, they do not cover all eventualities or possible developments in big data and AI. Hence, this report aims to be comprehensive in addressing potential ethical issues arising from the use of big data and AI in human biomedical research, including responsible data usage, data ownership, custodianship, and stewardship, data privacy, accessibility and security, data anonymisation and other ethical considerations and issues specific to AI in the subsequent chapters. The report will also take reference from existing data governance frameworks, where relevant, in developing its recommendations.

CHAPTER 6: RESPONSIBLE DATA USAGE

This chapter discusses the importance of ensuring responsible data usage in big data and AI use in biomedical research, and how researchers should manage data bias, and other incidental findings from big data research and mitigate the risks of discrimination from research participation, as well as manage and reduce the effect of unintentional biases arising from AI algorithms and models. The concept of social licence is also explained here.

6.1 Responsible data usage is concerned with ensuring that data is used lawfully, ethically, and in a fair and transparent manner without compromising data integrity. Responsible data usage seeks to protect individual privacy and data subject's autonomy, while also enabling researchers and society to acquire benefits from the use of big data and AI in biomedical research (see Chapter 3: Introduction and Chapter 4: The Promise of Big Data and AI Research Studies: Applications, Benefits, and Risks). It is important to support and promote the responsible use of data, as not doing so may lead to undesirable consequences such as the risk of harm to data subjects, discrimination or injustice, or inaccurate research outcomes stemming from bias in AI algorithms and the data used to train them, and in the larger societal context in which AI systems are used. Responsible use of data allows researchers and healthcare professionals to combine and analyse massive datasets, identify patterns or correlations, generate useful insights, and make faster and better data-driven decisions to improve research and health outcomes which in turn, helps to promote public trust and willingness to participate in biomedical research more generally.

6.2 While responsibility in data usage begins with researchers complying with existing legal and ethical requirements, nonetheless, in the context of Big Data and AI, there are additional considerations to factor into account given the eminent promise and potential increased risks, as laid out in the earlier chapters. The report deliberates on various ethical principles and their applications which would be important to inform research design and delivery in the context of Big Data and AI.

Issue 1 – How should we manage and use human biomedical research data responsibly to minimise as far as possible risks of harms and discrimination arising from participation or biases in biomedical research?

6.3 Structural inequalities and racial and group biases can be easily encoded in datasets, and the use of such inappropriate datasets in human biomedical research can reinforce existing social injustices and widen health inequalities, if not properly managed or used.[1]

Examples of biases in human biomedical research:

Genetic data of an individual who participated in genetic research or those of certain ethnic groups with genetic predispositions to specific genetic conditions could negatively impact their eligibility for insurance coverage, which is a form of harm as it sets back their important interests.

[1] Knight, H. E., Deeny, S. R., Dreyer, K., *et al*. (2021). Challenging Racism in the Use of Health Data. *The Lancet Digital Health, 3*(3), 144–146. https://doi.org/10.1016/S2589-7500(21)00019-4

Using AI in the classification of different skin lesions to aid clinicians in the diagnosis of skin cancers could lead to biases in the research. While most of the skin cancer cases are among the fair-skinned person population, people with darker skin can also develop skin cancer and are frequently diagnosed at later stages. Skin cancer represents 4-5%, 2-4%, and 1-2% of all cancers in Hispanics, Asians, and Blacks, respectively. Hence, deep learning frameworks validated for the diagnosis of skin cancer in fair-skinned people have a greater risk of misdiagnosing those with darker skin. In a recent study which trained a deep learning algorithm using dataset consisting of skin lesions from Asians, it reported an accuracy of 81% on the Asian testing set, and an accuracy of only 56% on the Dermofit dataset, which consists of skin lesions of Caucasian people.[2] The drop-in-accuracy signifies a lack of transferability of the learned features of deep learning algorithms across datasets that contain persons of a different race, ethnicity, or population.[3]

6.4 Responsible data usage in the development of AI tools, therefore, is important to reduce any social or ethnic bias that may become inadvertently embedded in machine learning models. One way to promote more unbiased models is to ensure that *training datasets* are inclusive and diverse across sociodemographic characteristics. If the incidence of specific conditions in certain groups is not sufficient to achieve equal distribution, then over and under sampling techniques may be used to achieve more balanced datasets for AI model training. Alternatively, large multicentre and multinational datasets can be assembled to provide diverse representation of disease conditions at the population scale. Another way to minimise bias is to test models or tools extensively on diverse *testing datasets* from across different sociodemographic groups or geographical boundaries. Such strategies help to minimise risk of social or ethnic discrimination arising from research participation, or discrimination, stigma and prejudice, or data biases in biomedical research and development.

6.5 In the context of big data and AI use in human biomedical research, the ethical principle of *justice* suggests that individuals, groups or communities should neither bear an unfair share of the direct burdens of participating in research, nor should they be unfairly excluded from the potential benefits of research participation. Therefore, researchers should strive to manage and use data in a way that does not create or reinforce biases to protect the welfare of participants and other individuals who may receive unfair treatment and experience inadvertent harm because of biased results. In the context of AI, this should be addressed by checking training datasets for the balance in representation of key attributes such as age, gender, ethnicity and socio-economic status. Equality of opportunity to take part is also crucial. Both overrepresentation and underrepresentation of various groups in research undermine the principle of fair inclusion of members of relevant populations and the need for appropriately inclusive and diverse datasets so as not to perpetuate unjust or inequitable outcomes in healthcare. For example, a 2020 study showed that many US FDA-approved medicinal drugs were mostly approved based on clinical trials

[2] Han, S. S., Kim, M. S., Lim, W. *et al*. (2018). Classification of the Clinical Images for Benign and Malignant Cutaneous Tumours Using a Deep Learning Algorithm. *Journal of Investigative Dermatology, 138*(7), 1529–1538. https://doi.org/10.1016/j.jid.2018.01.028

[3] Goyal, M., Knackstedt, T., Yan, S. *et al*. (2020). Artificial Intelligence-Based Image Classification Methods for Diagnosis of Skin Cancer: Challenges and Opportunities. *Computers in Biology and Medicine, 127*, 104065. https://doi.org/10.1016/j.compbiomed.2020.104065

conducted on men, and women were underrepresented, which could contribute to higher adverse drug reactions seen in women as sex differences in drug mechanisms were not considered in the research.[4]

6.6 The ethical value of *independent ethics review*, which is also an important consideration in research, dictates that the welfare, rights, and privacy of research participants are protected via IRBs or equivalent bodies which evaluate research protocols and ensure that appropriate care is taken such that the data used in research does not create or reinforce biases. To ensure consistency in decision-making and to uphold fairness and public trust, IRBs should apply similar ethical standards during their reviews to strive for fairness and promote public trust, by leveraging regulatory frameworks and appropriate definitions and metrics of fairness that mitigate risks of discrimination from research participation, or biases from big data studies (see examples below).

Examples of regulatory frameworks in place to mitigate risks of discrimination that arise from research participation and biases from big data studies:

Singapore – The '*Moratorium on Genetic Testing and Insurance* (2021)' is an agreement between the Ministry of Health (MOH) and the Life Insurance Association (LIA) which bans the use of all genetic test results from human biomedical research in insurance underwriting.[5]

UK – *'Code on Genetic Testing and Insurance (2018)'*: Similar to the Moratorium in Singapore, the UK Moratorium also bans the use of all genetic test results from human biomedical research in insurance underwriting.[6]

Issue 2 – How should institutions and researchers manage the return of incidental findings from big data research studies using personal medical data or findings generated from non-clinical grade data?

6.7 Incidental findings, in the context of human biomedical research, refers to potentially clinically significant findings of research participants with health or reproductive significance discovered in the course of conducting research but unrelated to the primary purposes, objectives or variables of the study.[7] The nature of big data research, with its high volumes of data and diverse velocities, varieties, collection protocols, processing, integration, and analyses, increases the likelihood of incidental findings and may make management of incidental findings more complex than those obtained from traditional data sources. In big data research, incidental findings can also be generated from non-clinical grade data that will require subsequent clinical-grade assessment. For example, incidental genomic variants of

[4] Zucker, I., & Prendergast, B. J. (2020). Sex Differences in Pharmacokinetics Predict Adverse Drug Reactions in Women. *Biology of Sex Differences, 11*(32). https://doi.org/10.1186/s13293-020-00308-5

[5] Moratorium on Genetic Testing and Insurance (2022). *Ministry of Health*. Retrieved November 23, 2022. https://www.moh.gov.sg/resources-statistics/moratorium-on-genetic-testing-and-insurance

[6] Code on Genetic Testing and Insurance (2022). *Association of British Insurers*. Retrieved November 23, 2022. https://www.abi.org.uk/data-and-resources/tools-and-resources/genetics/code-on-genetic-testing-and-insurance/

[7] FAQs on Human Biomedical Research Act (2021). *Ministry of Health*. Retrieved November 23, 2022. https://www.moh.gov.sg/docs/librariesprovider5/legislation/hbra-faqs.pdf

significance found on low pass sequencing used in research need to be confirmed with clinical grade sequencing specific to that gene. With the guidance of genetic counsellors, a confirmatory clinical sequencing test may be performed. If the presence of this gene is subsequently confirmed, patients may need to act on this information with advice from their doctors.

6.8 In such instances, non-disclosure of incidental findings may threaten the safety and welfare of data subjects, and may infringe on the ethical principles of transparency and accountability of data usage. There is, therefore, a duty and responsibility to consider the appropriate management or return of incidental findings by institutions and researchers. To guide the deliberations, the following ethical principles could be considered:

a. The principle for *respect for persons* requires that welfare and interests of data subjects and research participants should be duly protected and their right to make their own decisions without being coerced, misled or kept in ignorance should not be ignored. While it does not follow that consent will always be sought, this principle does require that account be taken of how data is used and any likely impacts on respect for persons to whom the data relates.

b. *Proportionality* considers whether the processes to achieve the goal of research are necessary and appropriate in relation to the research goal itself, and requires researchers to be cognisant of competing interests at hand (such as the consideration if the knowledge of the incidental findings offers more harm than benefit to the research participants, particularly if the incidental finding is non-actionable). Responsible research necessarily takes a defensible and proportionate approach to balancing these considerations.

c. *Transparency* and *accountability* suggest that, as a minimum, research participants are informed about how incidental findings will be managed, including their return if this option is part of a research protocol. Researchers and research institutions have to take into account that the non-disclosure of incidental findings may pose harm or threaten the safety of research participants when developing policies on the management of incidental findings, and act in the best interests of the participant.

6.9 The BAC recommended in its Ethics Guidelines for Human Biomedical Research (2021 revised edition)[8] that where there is a possibility that the research may yield clinically significant incidental findings, participants should be allowed to decide whether to be informed of such findings, during the consent taking process, prior to the commencement of the research. If a clinically significant finding is discovered, but the preference of the research participant receiving such information has not been specified, researchers should refer to their IRBs for advice on the appropriate handling of such information. The Human Biomedical Research Act (2015)[9] allows research institutions to develop and implement their own policy on whether research

[8] Ethics Guidelines for Human Biomedical Research (2021 Revised Edition) (2021). *Bioethics Advisory Committee*. Retrieved November 23, 2022. https://www.bioethics-singapore.gov.sg/publications/reports/bac-ethics-guidelines-2021

[9] Human Biomedical Research Act 2015 (2020 Revised Edition). *Singapore Statues Online*. https://sso.agc.gov.sg/Act/HBRA2015

participants should be re-identified and informed in the event of an incidental finding, research institutions must inform the IRBs and researchers of their policy on incidental findings. Researchers should inform research participants on the possibility of incidental findings arising from the research and seek their consent should any incidental findings be returned.[10]

Issue 3 – How should researchers/ developers ensure that data fed into the algorithm is not biased or result in bias-driven outcomes when developing AI algorithms?

6.10 The development of AI algorithms requires large datasets and it is important to ensure that datasets used are not biased. Inherent bias in datasets may result in inaccurate or skewed conclusions or disproportionally impact marginalised or vulnerable groups and increase the risk of discrimination as highlighted in issue 1. Hence, robust development with a view to ensuring fair representation, and rigorous assessment of *fairness of outcomes* are key considerations for AI tools in biomedical applications.

6.11 *Auditability* or having an audit mechanism in place, enables researchers, developers, and organisations to track AI behaviour and monitor its usage which underpins the ethical principles of promoting *transparency* and *accountability*. Such audit processes look into the assessment of AI design (patient cohort selection, model selection), development (algorithm, hyperparameter selection and model validation), evaluation (one-time evaluations on diverse test sets as well as ongoing characterisations of performance) and deployment (model interpretability) and are exceptionally important in applications or cases where decisions made by AI algorithms affect the rights, safety and health of individuals. Auditability also ensures compliance of AI with the best technical, regulatory, and ethical practices at each stage of its life cycle. Alan Turing Institute, the UK's national institute for data science and AI, has proposed a comprehensive three-tiered approach[11] consisting of (i) Support, Underwrite, and Motivate (SUM) values, which serves as guiding principles throughout the entire innovation process and offer an accessible ethical framework for evaluating the ethical acceptability of a potential project and its ethical consequences; (ii) Fairness, Accountability, Sustainability, Transparency (FAST) Track principles which function as a set of principles that enable an actionable approach to the ethical development and use of big data and AI systems, assisting developers and users to implement ethical standards in practice during the innovation process; and (iii) Process-Based Governance (PBG) Framework which comprises of both technical and non-technical tools such as processes, procedures, guidelines, and records that assist developers and users to implement ethical values and principles in practice. The FAST Track principles help to mitigate bias, ensure non-discriminatory, and fair processes are in place and safeguard public trust through delivering safe and reliable AI innovation. The PBG Framework facilitates developers in setting up transparent processes of design and implementation that safeguard and enable the justifiability of the AI project/product.

[10] FAQs on Human Biomedical Research Act (2021). *Ministry of Health*. Retrieved November 23, 2022. https://www.moh.gov.sg/docs/librariesprovider5/legislation/hbra-faqs.pdf

[11] Leslie, D. (2019). Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems in the Public Sector. *The Alan Turing Institute*. https://doi.org/10.5281/zenodo.3240529

6.12 To avoid introducing data bias to AI algorithms, the ethical principle of *justice* as equal treatment and health equity should be considered so that AI systems developed for use in human biomedical research are designed in a way that they do not create or reinforce bias, and that care should be taken to apply appropriate standards of data quality when developing AI algorithms. Assessment of potential data biases could be addressed by leveraging suitable robust mechanisms to prevent biases or ensure sufficient removal of biases.

6.13 *Explainability* and *justifiability* are additional concepts specific to AI development for researchers to keep in mind for research studies involving AI (see Chapter 13: Ethical Considerations and Issues Specific to AI).

Issue 4 (related to issue 3) – How could researchers and developers manage and reduce the effect of unintentional biases arising from AI algorithms and models despite safeguards in place?

6.14 To manage and reduce the effect of unintentional biases arising from AI algorithms and models, researchers and developers should check for relevant unintended biases even if safeguards had been put in place. For example, a study on 'Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) which is a software used to predict recidivism in Broward County, Florida, showed incorrectly labelled African-American defendants as 'high-risk' of re-offending or committing another crime at nearly twice the rate of mislabelled white defendants. A technology company discontinued the development of a hiring algorithm based on analysing previous decisions after discovering that the algorithm penalised applicants from women's colleges. Another study also found error rates in facial analysis technologies differed by race and gender.[12] The effect from unintentional biases mentioned in these examples could be reduced by testing all AI tools, algorithms, and models across data with variations across characteristics such as age, gender, ethnicity, socio-economic status, and education.

6.15 Researchers and developers have the responsibility to identify and minimise the effect of unintentional biases and mitigate risks from AI development. This obligation is supported by reflecting on the ethical considerations of *justice, consistency, transparency,* and *accountability* (discussed in issue 3) and how these would apply. Researchers and developers should consider regular review (including pre-processing of data) and validation of data, algorithms and models used for human biomedical research to maintain accuracy and fairness, and to minimise any unintentional biases. This may be achieved with innovative training techniques such as using transfer learning or decoupled classifiers for different groups. These methods have been proven to be useful for reducing discrepancies in facial analysis technologies. Performance of AI in hypothetical situations can also be tested via tools such as Google's 'What-If Tool', which visually examines the behaviour of trained machine learning models.[13]

[12] Buolamwini, J. & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, in Proceedings of Machine Learning Research, 81,* 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

[13] Google, People + AI Research (2022). What-If Tool. *Google Research.* Retrieved November 23, 2022. https://pair-code.github.io/what-if-tool/index.html#about

Issue 5 – How could researchers and developers leverage on AI systems and algorithms to eliminate or reduce existing bias and improve decisions in ensuring responsible data usage?

6.16 In ensuring responsible data usage, researchers and developers could also actively leverage the potential of AI to ethically improve decisions by eliminating or removing existing bias that reflect the larger societal context in which AI systems are used.[14]

6.17 Researchers and developers must responsibly take advantage of the several ways that AI can improve on traditional human decision-making. For example, AI algorithms can help to reveal intrinsic human-led biases in the system, because AI focuses only on variables that accurately predict outcomes from the available data, which is different from humans who might not be able to identify the factors that led to their decisions, such as the choice to hire or ignore a particular job candidate. Furthermore, it may be easier to probe algorithms for bias via programming, which would provide greater transparency and clarity regarding the factors and motivations behind decisions. This allows researchers and developers to uncover discriminatory practices and human biases that were previously unknown or unproven. In addition, AI can be leveraged to reduce the impact of discrimination and biases and improve decision-making for traditionally marginalised groups, also termed by researchers as ‘disparate benefits from improved prediction’.[15]

6.18 Researchers and developers should also be trained in relevant topics such as unconscious bias in machine learning models to understand the impact and consequences of such bias and learn ways to reduce risk of discrimination or injustice, or inaccurate research outcomes stemming from bias within AI algorithms. Such training would help to improve decision-making and ensure responsible data usage.

Issue 6 – What is ‘social licence’ and what is its ethical significance for responsible biomedical research using big data and AI?

6.19 ‘Social licence’ refers to the ongoing acceptance within a community or wider society of a company or industry’s standard business practices and operating procedures. It can include informal permissions granted by employees, stakeholders, and the general public (i.e., in the form of community support, successful collaborative partnerships, employee loyalty, stakeholder investments) to institutions, governments or corporations to carry out a particular set of activities. Social licence emphasises on the need for corporations and institutions involved in activities that are likely to elicit public discomfort to behave in a trustworthy and responsible manner, in addition to complying with legal requirements. Action beyond the boundaries of the public’s collective social approval would likely result in corporate damage and reduction in public trust.[16]

[14] Manyika, J., Silberg, J., & Presten, B. (2019). What Do We Do About the Biases In AI? *Harvard Business Review*. Retrieved February 23, 2023. https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai

[15] Kleinberg, J., Ludwig, J., Mullainathan, S. *et al*. (2018). Discrimination in the Age of Algorithms. *Journal of Legal Analysis, 10,* 113–174. https://doi.org/10.1093/jla/laz001

[16] Carter, P., Laurie, G. T., & Dixon-Woods, M. (2015). The Social Licence for Research: Why ‘care.data’ Ran into Trouble. *Journal of Medical Ethics, 41*(5), 404–409. https://doi.org/10.1136/medethics-2014-102374

6.20 In the context of big data and AI use in biomedical research, ‘social licence’ can help to promote public trust. This is achieved through a series of actions including public consultation, incorporating views of various stakeholders, establishing robust processes, implementing policies by regulatory bodies and oversight by third parties. When the public views a particular entity as trustworthy, the entity is also more likely to have social licence to engage in research activities such as the collection and use of personal data.[17] In such instances, ‘social licence’ can help to engender trust among the public and facilitate their acceptance on the use of data by the trusted entity for research. It would also render the entity using the data accountable to the upholding of the terms and conditions of data usage as initially communicated.

6.21 Studies have shown that many people are supportive of their health-related data being shared to support research and public health policy when the data is used for public good, in transparent ways, and by trusted institutions.[18] While trust and support for public institutions accessing health-related data can be reasonably expected from the public in certain socio-political contexts, the same social licence may not be accorded for private-public partnerships where commercial entities access personal, health or medical data for research.

Example of private-public partnership:

An example can be observed in UK’s ‘care.data Initiative’ in 2013, a public-led initiative that aimed to promote private-public partnership and to collate data from primary care practices across the country. Though promising, this initiative subsequently failed and was abandoned as a result of resistance from health care providers and the public. Issues with patient anonymity, opt-out choices, unclear criteria for health data access and a general mistrust of commercial interests with the collected data were cited.[16] The loss of a ‘social licence’ may have led to the failure of this initiative.

6.22 Whilst commercial partnerships yield benefits such as enabling the development of new drugs and treatments, individuals’ mistrust of the private sector is commonplace, especially where these commercial entities might be perceived as exploitative or profit-driven without due consideration of the following issues to ensure social licence for private-public partnerships:

a. Transparency: It is essential to have transparency in how data is collected, used, and shared in the public-private partnership. This includes informing the public of the types of data being collected and how it will be used which ensures data quality and keeps the process credible and transparent.

b. Consent: Consent is a critical component in any partnership involving personal data. The partnership should ensure that the data subjects have given their informed consent to the use of their data in the research.

[17] Gehman, J., Lefsrud, L. M., & Fast, S. (2017). Social Licence to Operate: Legitimacy by Another Name? *Canadian Public Administration, 60*(2), 293–317. https://doi.org/10.1111/capa.12218

[18] Kalkman, S., van Delden, J., Banerjee, A. *et al* (2019). Patients’ and Public Views and Attitudes Towards the Sharing of Health Data for Research: A Narrative Review of the Empirical Evidence. *Journal of Medical Ethics, 48*(1), 3–13. https://doi.org/10.1136/medethics-2019-105651

c. Privacy: Data privacy is an important concern for the public, and any partnership must take into account the need to respect individuals' privacy rights. Appropriate measures should be taken to safeguard the confidentiality of personal data, including implementing data security measures and data anonymisation where possible.

d. Ethics oversight: The partnership should be guided by ethical principles (see para 6.22), including respect for the rights and dignity of the data subjects. Any research involving human subjects should be reviewed and approved by an institutional ethics review committee (i.e., IRBs)

e. Accountability: Accountability is essential to build trust with the public. The partnership should be accountable for the data they collect and use, and they should be transparent about their decision-making processes.

f. Benefits to society: It is essential that the partnership generates benefits to society, such as advancing scientific knowledge, improving patient outcomes, or providing economic benefits.

g. Stakeholder engagement: Involving stakeholders, including patients, patient advocacy groups, and the public, in the partnership's decision-making processes can help build trust and ensure that the partnership is responsive to societal needs.

6.23 While commercial practices may sometimes be even more responsible in certain situations than public sector practices and generate products of greater public value, it is still important to address societal and individual negative perceptions and potential mistrust of commercial entities through transparency in processes and demonstration of trustworthiness actions and responsible behaviours. Many countries adopt a more stringent view towards regulating the commercial use and collection of biomedical and health data as compared to the clinical and/or research use of biomedical and health data. Examples of countries with legislations and frameworks in place to prevent the commercial misuse of health data, such as the Health Insurance Portability and Accountability Act (HIPAA)[19] in the US; General Data Protection Regulation (GDPR)[20] in Europe (applies to all processing of data, not just for commercial use); and Personal Data Protection Act (PDPA)[21] in Singapore. Other than legislative frameworks, ethical guidance and standards are developed to guide the development or commissioning of AI products. The key recommendation on the use of data in private-private partnerships is to obtain consent for the use of data, and/or to deidentify or anonymise data according to the data protection frameworks, and to ensure that appropriate contracts are put in place that spell out the rights and responsibilities of both parties in the use of the data.

[19] Your Rights Under Health Insurance Portability and Accountability Act (HIPAA). (2022). *U.S. Department of Health and Human Services (HHS).* Retrieved November 23, 2022. https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

[20] EU General Data Protection Regulation. (2022). *GDPR.eu.* Retrieved November 23, 2022. https://gdpr.eu/tag/gdpr/

[21] Personal Data Protection Act 2012 (2020 Revised Edition). *Singapore Statues Online*. https://sso.agc.gov.sg/Act/PDPA2012

6.24 Following the concept and use of 'social licence' in big data and AI applications in biomedical research to demonstrate trustworthiness and to promote public trust, as well as facilitating acceptance on use of data for research among all entities involved in the data handling process, some key ethical principles including *respect of persons, solidarity,* and *accountability* can assist in the pursuit of social licence:

a. The principles of *respect for persons and transparency* require that entities convey to research participants the partners involved in the research studies, how the data will be used, shared or accessed and obtain informed consent from them accordingly. This principle also mandates the respect for privacy, safeguarding of confidentiality, and minimising of harm to research participants. The use of opt-outs, where possible, allow members of the public to retain a degree of control over how their data is used.

b. The principle of *solidarity* advocates a balance between the interests of individual and wider society, and reflects the importance of the promotion of general altruism and other pro-social motives in participation in biomedical research. It is important to seek an acceptable equilibrium of individual's interests and the collective interests or national needs (e.g., population trends that improve diagnosis). To ensure responsible data use and achieve social licence, organisations must demonstrate a commitment to engage the stakeholders and public and consider their needs and concerns, especially individuals whose data is being used, and to ensure that the benefits and risks of data use are being distributed fairly, equitably, and inclusively.

c. *Accountability* requires that entities including individuals, public and private institutions are held responsible for their processes, decisions, and actions. Appropriate audit mechanisms and processes should be put in place to ensure data integrity and transparency. Such audit mechanisms will engender public trust and garner social approval. The immediate goal should be to demonstrate trustworthiness of action, i.e., giving citizens good reasons to trust institutions and how their data is used. This gives the best change of generating social licence.

CHAPTER 7: DATA OWNERSHIP, CUSTODIANSHIP AND STEWARDSHIP

This chapter discusses data ownership, custodianship, and stewardship in the context of big data and AI use in biomedical research. Intellectual property rights, international research collaborations and data regulatory frameworks are also discussed.

Data Ownership

7.1 The concept of data ownership has traditionally been debated from the legal standpoint and there is a difference in how various legal frameworks are applied to data ownership.[1] Indeed, the dominant view in legal theory asserts that data cannot be owned (with the exception of the intellectual property system). Nonetheless, in the context of big data and AI use in biomedical research, data ownership may be referred to as legal rights or the exclusive personal or proprietary rights conferred by law, to have complete control and autonomy over a single or set of data elements.[2] Personal rights, such as those relating to the protection of one's own body or one's own character, reputation and identity, are intrinsic and absolute, while proprietary rights over 'things' may be transferrable. From a legal standpoint, current legal frameworks are incompatible with the idea of data ownership.[3] However, the language of 'data ownership' is widespread in the international biomedical community and any claims to data ownership may impact access to health and patient data, and this would in turn affect biomedical research, limit individual freedom and result in economic trade-offs. Hence, any appeals to data ownership within the biomedical sphere need to be reviewed in the context of the use of big data and AI in biomedical research.

7.2 In Singapore, the individual does not have the proprietary right or interest in the information contained in his or her medical records at common law.[4] This is similar to the English common law position that the appropriation of data or facts is not protected by copyright law.[5] In terms of Intellectual Property (IP) rights over data, while the Singapore Court of appeal in Global Yellow Pages has recognised copyright protection where there is sufficient creativity in the selection of arrangement of the data in the compilation, the data or facts themselves are not protected by copyright law. Singapore does not have a sui generis database right[6] unlike England and Europe and the Singapore Court has declined to adopt such a right at common law. The relevant laws in Singapore that protect health data would include the Personal Data Protection Act (PDPA) 2012, the Human Biomedical

[1] Law Reform Committee, Singapore Academy of Law. (2020). Rethinking Database Rights and Data Ownership in an AI world. *Singapore Academy of Law.* (2020, July) Retrieved January 16, 2023. https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020%20Rethinking%20Database%20Rights%20and%20Data%20Ownership%20in%20an%20AI%20World_ebook_0_1.pdf

[2] Ballantyne, A. (2020). How Should We Think about Clinical Data Ownership? *Journal of Medical Ethics, 46*(5), 289–294. https://doi.org/10.1136/medethics-2018-105340

[3] Liddell, K., Simon, D. A., & Lucassen, A. (2021). Patient Data Ownership: Who Owns Your Health? *Journal Of Law and The Biosciences, 8*(2), 1–50. https://doi.org/10.1093/jlb/lsab023

[4] Chan, G. K. Y. (2021). Health Law and Medical Ethics in Singapore (1st edition). (pp. 154). Routledge.

[5] SGCA 28. (2017). Global Yellow Pages Ltd v Promedia Directories. Point [34]. *Singapore Courts – Judgements and Case Summaries.* https://www.elitigation.sg/gd/s/2017_SGCA_28

[6] Sui generis 'database rights' were created by the EU Directive 96/9/EC and the UK Copyright and Rights in Databases Regulations 1997

Research Act (HBRA) 2015, the Healthcare Services Act (HCSA) 2020 and the National Registry of Diseases Act 2007. Singapore Medical Council's Ethical Code and Ethical Guidelines (2016)[7] further imposes confidentiality requirements on medical professionals. Research participants have no claims to IP rights over data about themselves whereas researchers and research institutions using their data and generating valuable datasets, new products and novel therapies will be able to secure IP.

7.3 Given the increasing value of data and its use in AI, we recognise the need to ensure responsible use and access to big data as well as recognising the time and effort that is required to create and curate datasets for biomedical research. Ethical considerations on appeals to data ownership may help provide clarity in terms of how data use and access should be managed (i.e., the idea that the 'data owner' decides how his/her data is used or accessed), and also may reveal what underlies property-type claims over data and datasets. Furthermore, given that big data is often derived from multiple sources and analysed to generate other datasets internationally, the jurisdictions in which 'data ownership' may apply would be less clear and it would be important to focus on 'who has the responsibility to curate the data' and 'who has the right to use the data', rather than 'who owns the data' to ensure responsible data use and access. This is a matter of best ethical practice. However, as a matter of law and assuming that the data owner could be identified, it is important nonetheless to emphasise that data owners have significant responsibilities to ensure that the data is secured, appropriately assigned, accessed and disposed of. This contrasts with data custodianship, which is an assignment of responsibility by the data owner to the custodian to manage the use and access to the data.

Data Custodianship

7.4 Data curation and custodianship are two sides of the same coin. Data custodianship refers to the maintenance of information, data systems, and the safe custody, transfer, storage and use of data.[8] Data custodians have a responsibility to establish and maintain social licence in the use of personal information in biomedical research. Personal information, including health information, shared by patients in the course of biomedical research are regarded as sensitive and therefore necessitate safeguards in place to ensure confidentiality, robust data protection, and responsible use. Data custodians act on behalf of institutions to authorise the disclosure/release of individual's personal information for research needs and are responsible for ensuring that the disclosure/release of data complies with legal, ethical and policy requirements. While research institutions do not own these data per se as there are no IP rights over the raw data, nonetheless, as individuals entrust these institutions with their personal information, it is important that this trust is not breached, and data custodianship can play a key role in helping to ensure this.

[7] Ethical Code and Ethical Guidelines (2016 edition), Section C7: 'Medical Confidentiality'. *Singapore Medical Council*. https://www.healthprofessionals.gov.sg/docs/librariesprovider2/default-document-library/2016-smc-ethical-code-and-ethical-guidelines---(13sep16).pdf

[8] Allen, J., Adams, C., & Flack, F. (2019). The Role of Data Custodians in Establishing and Maintaining Social Licence for Health Research. *Bioethics*, *33*(4), 502–510. https://doi.org/10.1111/bioe.12549

7.5 Data custodianship can help maximise benefits and minimise costs of biomedical research. Good data custodianship comprises putting in place mechanisms to promote the responsible and ethical use of data, protecting the privacy of individual data, and ensuring data security. This enables progress whilst not overly increasing the costs of biomedical research. As such, it may be in the institutions' best interests to act as a 'data custodian' in the long term, safeguarding personal information and protecting individual's data privacy and maximising overall benefits to the public.

Data Stewardship

7.6 Data stewardship entails an appropriate and responsible approach to the collection, management, and promotion of responsible use of data, particularly those that may identify individuals.[9] It includes overseeing all aspects of the data lifecycle – creating, preparing, using, storing, archiving, and deleting of data, in accordance with an organisation's established data governance principles to ensure data quality and integrity. Stewardship and custodianship are complementary roles; they are similar, but not identical.

7.7 While data custodianship tends to focus on the safe keeping of data (i.e., safe custody and storage), data stewardship is concerned with the safe management of the data resource as a whole and involves the coordination with multiple parties and may also include the development and implementation of policies for managing and sharing data (i.e., 'safe data' are made available to third parties through stewardship) with responsible third parties for use in the interests of biomedical research, as well as the training and educating of stakeholders about the importance of responsible data management.[10] Stewardship of patient and clinical data supports biomedical research by ensuring that private and confidential information garnered from patients and individuals are protected and used appropriately, providing assurance to contributors of data confidentiality and thereby improving healthcare through advancements in biomedical research in the long term. In the big data context, data stewardship for responsible use will involve overseeing governance mechanisms across different data ecosystems, for example, when data from different sectors are linked, transferred and used for research purposes.

Issue 1 – How much control/rights/power do individuals have after contributing their data for biomedical research?

7.8 Individuals may consider data contributed to biomedical research to be personal and therefore may seek to claim ownership and rights over it. However, from the legal perspective, patients do not own their data but are nevertheless entitled to have their concerns regarding the use of their health data considered and addressed by virtue of their personal interests.[11] The underlying rationale leading to claims of data ownership may include privacy protection to prevent unjustified or unauthorised use

[9] Kanaan, S. B. & Carr, J. M., M.D. (2009). Health Data Stewardship: What, Why, Who, How – An NCVHS Primer. *National Committee on Vital and Health Statistics*. Retrieved January 16, 2023. https://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090930lt.pdf

[10] Fan, Z. (2019). Context-Based Roles and Competencies of Data Curators in Supporting Research Data Lifecycle Management: Multi-Case Study in China. *Libri, 69*(2), 127–137. https://doi.org/10.1515/libri-2018-0065

[11] Liddell K., Simon, D. A., & Lucassen A. (2021) Patient Data Ownership: Who Owns Your Health? *Journal of Law and the Biosciences, 8*(2), 1–50. https://doi.org/10.1093/jlb/lsab023

or access, control over potential and informed uses of the data (including secondary uses) as well as a desire to have a share of benefits generated from the use of the data in biomedical research.

7.9 Some academics are in favour of a broader reach of ownership that takes into account that various stakeholders are involved in the research project and suggest that the solution to potential data harms (e.g., privacy breaches, discrimination and stigma, disenfranchisement, disempowerment and exploitation) could involve strategies to reconnect patients with their data and engage them in debates and decision-making about secondary uses.[3] However, there are multiple legal and practical challenges with this approach. Most particularly, enabling only patient control of data does not necessarily prevent against potential harms. Instead, addressing potential data harms through data stewardship and/or the use of custodians is increasingly presented as a solution to various concerns about data use such as withdrawal from data sharing and collection when researchers overstep their social licence or are perceived to have done so. This relies less explicitly on interpretation of data ownership as a private property, and in doing so can still reach the objective of protecting against harms. Thus, in this report the approach that is preferred is not to focus on data ownership and control, and rather to explore responsible data use.

7.10 To guide responsible data use, design and development of AI and in furthering collaborations/partnerships between research and healthcare institutions, the following ethical principles should be considered:

a. The principle of *respect for persons* requires that research institutions and researchers take into account the welfare and concerns of individuals whose personal data is used, even if the individuals do not legally own the data. Research institutions and researchers should respect individuals' right to withdraw, as far as possible and practicable. However, there are exceptions to the right to withdraw as stipulated under sections 14(2) and 14(3)[12] of the HBRA 2015, where the withdrawal of consent in specified circumstances, does not affect the research information obtained before the consent is withdrawn and such information may be retained and used for the research. For instance, a donor of human tissue or research participant who is authorised to give consent, may at any time, withdraw the consent to the use of the donor's tissue for research if the tissue is individually-identifiable and has/has not been used for the research but it is practicable to discontinue further use of the tissue for the research.

b. The principle of *justice* mandates that the individuals whose personal data is being used are not denied access to the benefits of the biomedical research, if it is possible to offer the benefits to them.

c. The principle of *stakeholder engagement* requires that research institutions and researchers consider the views and feedback of individuals and other stakeholders when using or accessing personal data in biomedical research, and/or when developing AI algorithms or models. This helps to ensure that

[12] Human Biomedical Research Act 2015 (2020 Revised Edition), Sections 14: 'Withdrawal of Consent'. *Singapore Statutes Online*. https://sso.agc.gov.sg/Act/HBRA2015

individuals and other stakeholders' welfare and interests are sufficiently protected.

d. *Accountability* requires that researchers and research institutions conduct biomedical research with the highest ethical standards and take responsibility for their actions and decisions. This includes informing research subjects on how their data is used and accessed and how data or AI algorithms may be used to inform decisions.

Issue 2 – What are the responsibilities of a data custodian?

7.11 Data custodians could be individual practitioners, research institutions, hospitals, persons or organisations who exercise control over researchers' access to data and regulate the use of their data collections to ensure sustainability and the scientific, ethical and legal correctness of their use. Data custodians also ensure that access requests comply with the applicable legislation and the conditions stipulated in the consent form or data sharing agreement of research participants.[13] In addition, 'social licence' arises when a community or group considers a particular practice acceptable, hence it becomes a core responsibility of data custodians to behave in ways to attract such social licence as the pursuit of biomedical research relies on the existence of such social licence.

7.12 Data may be held in a centralised database or source (e.g., hospitals and clinics), multiple sources or decentralised platforms such as digital health mobile applications or combined data repository such as:

a. The National Electronic Health Record (NEHR) system which enables clinicians and healthcare professionals to view patient health records across the national healthcare network and different healthcare providers; and

b. Online portals such as HealthHub which is a national digital healthcare platform that allows individuals to access their personal medical records, links to healthcare services and institutions and related information and tools.

7.13 These different data sources may influence the responsibilities of the relevant data custodian:

a. With regard to data held in a <u>centralised source</u>, such as a hospital, the data custodian is required to adhere to the laws (including the new Health Information Bill (to be enacted) and regulations that apply to the collection, use, access and management of data in the premise and is also subject to contractual obligations in consent forms or data sharing agreements.

b. Data custodians managing data from <u>decentralised platforms</u>, such as social media or health apps, may be subject to myriad laws and regulations that cut across sectors and also the expectations and preferences of the platforms'

[13] Rosenbaum, S. (2010). Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. *Health Services Research*, *45*(5 Pt 2), 1442–1455. https://doi.org/10.1111/j.1475-6773.2010.01140.x

users. The consent models for collection, use, management, and access of data from various decentralised platforms or sources may also differ. Data custodians should consider how they can comply with various laws and consent models, including the present guidelines governing the access to and use of human biomedical research data in Singapore. They should be clear about who has the right to grant data access to requestors, and whether all parties are protected by the governing conditions.

c. Data custodians managing AI models built from data may face challenges including their powers to control personal data which underlies issues with data interoperability and access to health information, and the risk of re-identification of personal data. While regulatory and legal regimes might cover a number of different sectors within and beyond health, the data sharing cultures, conventions, best practices and expectations might be different between these sectors. As such, the data custodian should stay up to date with the latest developments of big data and AI use in biomedical research and seek to ensure safe data custody and storage across all sectors that are involved; this includes a responsibility to check that data processes are compliant with the relevant regulatory frameworks in place. Data stewards also play a key role by ensuring data access, security, quality, and that data governance are upheld by monitoring and determining the efficacy of data governance regimes, irrespective of the sector or sectors in which they operate.

7.14 When using multiple data sets and data platforms as will often be the case in big data research, the following ethical principles may be considered in setting out the roles and responsibilities of data custodians:

a. *Respect for persons* and *stakeholder engagement* require that research participants' welfare and concerns are taken into consideration during the conduct of biomedical research or development of AI models and algorithms, and their data is stored securely and used or accessed in accordance with the conditions set out in the research agreement. It is important to note that respect for persons does not always mean that consent is sought. Sometimes this is not feasible or can undermine the research objective. Respect can still be forthcoming, however, when data has been anonymised and is no longer individually-identifiable. Singapore's Personal Data Protection Commission (PDPC) Advisory Guidelines for the Healthcare Sector stipulates that anonymised datasets that do not relate to any identifiable individual will not require consent before use. [14]

b. *Proportionality* requires that custodians factor in the risks and benefits to all parties involved when considering whether, when, and how to grant access to data. This involves full risk assessment of sharing and using data across different platforms, especially when standards and governance mechanisms might differ.

[14] Personal Data Protection Commission (PDPC) Advisory Guidelines for the Healthcare Sector (2017 revision), Part II, Section 2: 'Collecting, Using, or Disclosing Personal Data for Purposes Other Than for the Patient's Visit or Medical Care'. *Personal Data Protection Commission Singapore*. https://www.pdpc.gov.sg/guidelines-and-consultation/2017/10/advisory-guidelines-for-the-healthcare-sector

c. *Accountability* requires that the conditions governing the access to, and use of such data is scrutable by data stewards who ensure the implementation of proper data governance. Data stewards are ultimately responsible for setting data quality metrics and requirements, such as the acceptable values, ranges, and parameters for each data element. They also assist to set up procedures for finding and resolving problems with data quality.

Issue 3 – Does a person who has provided biological materials and/or data, but did not participate in the subsequent processing and/or analysis, have IP rights in the data?

7.15 The question of whether research participants, from whom the data was obtained, are entitled to any part of the rights to any IP that the researchers or research institutions have subsequently developed, remains controversial. In Singapore, individuals are not conferred any IP rights over their personal health data. Such health data include any and all information generated or collected in any form, electronic or non-electronic, relating to individuals who participated in a biomedical research programme. Datasets or novel products invented using health data might, however, be subject to a range of IP rights controlled by the research institutions who do 'work' using the original raw data.[5] IP rights arise when new 'work' is done on raw data to create something new, such as a novel invention or a new dataset. No property exists in the raw data themselves. IP is attributed to those persons or institutions who do this 'work', e.g., through research techniques or technical manipulation of data. Research subjects are not considered to do sufficient work to generate IP rights for themselves.

7.16 Classification of research data depends on the type of data collected and how and who has been allowed access to it. Data that may not be distinguishing enough for identification of a person may be less useful for population studies, yet health data often do not just comprise an individual's data but also details about other family and non-family members. Generation of data is also often not carried out solely by the research participant but by multiple different parties and devices which may convolute the contribution to IP rights in the information that becomes valuable for biomedical research purposes. Organisations should take into consideration the ethical principles of *justice* by ensuring fairness, and *transparency* as well as the need to obtain trust and consensus from the contributor of the data, as far as possible. In smaller scale data projects, specific and formal agreements should be put in place to delineate the risks and expectations of all parties so that research participants are informed on whom the data was collected and the method of data collection. A well-known example is the IP controversy surrounding the use of cancer cells derived from patient 'Mdm Henrietta Lacks' in the 1950s, from whom the 'HeLa' cell line was derived. Mdm Henrietta Lacks and her family were not accorded any IP rights for the development of the HeLa cell line. The controversy continues until this day. Though the collection and use of patients' cells in research without consent was a commonly accepted legal practice in the 1950s, such a practice is not acceptable today.[15] However, this does not negate the need to discuss the position on data IP rights, and in particular to be clear that while IP will not arise for participants or their family it might accrue to researchers and institutions who use the raw data to

[15] Johns Hopkins Medicine. (2022). The Legacy of Henrietta Lacks. *Johns Hopkins Medicine.* Retrieved January 16, 2023. https://www.hopkinsmedicine.org/henriettalacks/

generate valuable biomedical datasets or new products or therapies. The following ethical principles may be useful to guide the considerations:

a. While it is uncertain in Singapore whether a person, or a body corporate, can legally own human biological materials or whether the donor can have any property rights over his or her biological materials after it is contributed for research, the general common law position is that a person does not 'own' his body or any part of it.[16] However, this is subject to common law developments, legal claims and the legislative framework for human tissues and organs in the HBRA 2015[17], the Human Organ Transplant Act (HOTA) 1987[18] and the Medical (Therapy, Education and Research) Act (MTERA) 1972.[19] It is also an offence to trade in organs and tissues under HOTA and HBRA and the human body or any parts of it should not be used as a means for financial gain. Thus, the donation of biological materials for use in research should be considered as an altruistic gift, where the altruistic donor does not possess IP rights in any development arising from the research, and donations should be made and accepted on that understanding.[20] Even though there may be no IP rights for research participants, the principle of *respect for persons* advocates for the rights of those persons to receive comprehensive information about the purpose, nature, and potential risks and benefits of the research, and to be allowed to make an informed decision on their participation in biomedical research. Although health data is different from biological materials, the understanding of the act of contribution of data for biomedical research as an altruistic gift is the same as the understanding of donation of biological materials for biomedical research.

b. The principle of *justice* requires researchers to distribute the benefits and burdens of research fairly and equitably among all relevant stakeholders, including research participants, researchers, and society. Though data and biological materials are contributed or donated altruistically, the nature and extent of the research participants' contribution should be taken into account in deciding how benefits arising from the biomedical research and any IP generated by the researchers is shared.

c. The principle of *solidarity* reflects the importance of altruism as a basis of participation in biomedical research, where the common interest/societal benefits are emphasised. While researchers or research institutions own the IP rights, they should balance individual interests (i.e., reaping the earnings from their IP) against the wider societal interests by maximising the rewards of their

[16] Chan, G. K. Y. (2021). Health Law and Medical Ethics in Singapore (1st edition), 244–252. Routledge.

[17] Human Biomedical Research Act 2015 (2020 Revised Edition), Section 32: 'Commercial Trading of Human Tissue Prohibited', and Section 33: 'Advertisements Relating to Commercial Trading of Human Tissue Prohibited'. *Singapore Statues Online.* https://sso.agc.gov.sg/Act/HBRA2015

[18] Human Organ Transplant Act 1987 (2020 Revised Edition), Section 13: 'Buying or Selling of Organs or Blood Prohibited and Void', and Section 14: 'Advertisements Relating to Buying or Selling of Organs or Blood Prohibited'. *Singapore Statues Online.* https://sso.agc.gov.sg/Act/HOTA1987

[19] Medical (Therapy, Education and Research) Act 1972 (2020 Revised Edition), Part 2: 'Anatomical Gifts'. *Singapore Statues Online.* https://sso.agc.gov.sg/Act/MTERA1972

[20] Bioethics Advisory Committee. (2021). Ethics Guidelines for Human Biomedical Research (2021 Revised). *Bioethics Advisory Committee*. Retrieved April 18, 2023. https://www.bioethics-singapore.gov.sg/publications/reports/bac-ethics-guidelines-2021

research for the benefit of society and making their research findings more widely accessible for the general public. For instance, some researchers earn revenue by licensing their big data and AI models built from participants' data to commercial companies. However, by allowing open source for their big data and AI algorithms, this will benefit fellow academics and non-commercial public users and incentivise individuals to step forward to contribute data for research, bringing benefits to the wider community.

Issue 4 – How should international research collaborations that involve the use and sharing of large volumes of biomedical data across countries be managed?

7.17 Collaborative projects taking place across borders are common where researchers are able to gather and complement their expertise to effect more meaningful outcomes in biomedical research and contribute to the advancement of medicine.[21] Ample data is required to continue advancing medical research and scientific progress, and cannot be done in silos. Increasingly, big data and AI in biomedical research has become an international endeavour where there is value in data-sharing across borders, but attention has to be placed on cultural nuances, jurisdiction, policy, data comparability, technical, and practical challenges in making these data shareable and interoperable internationally.[22] Different countries have different laws and regulations with regard to research project approvals, research governance, processes to deal with regulatory breaches, and traditions and cultures regarding the sharing of data. This is particularly relevant since research data sets are becoming so large that it is difficult to move or copy data from one place to another and analysis is increasingly done where the data is sited, instead of porting data over for analysis. This is also true for data security reasons, where data is best processed at the site at which it was collected and processed (e.g., the use of 'Data Safe Havens'[23] discussed in Chapter 8: Data Privacy, Accessibility and Security). In addition, there are scientific-political reasons for researchers not wanting to share their data (e.g., control of data access and data ownership). As such, copious amount of research data is typically processed locally, and local data regulations must be understood and adhered. To encourage international research collaborations that involve the use and sharing of large volumes of biomedical data across countries, it is important to establish data governance principles for promoting data quality, integrity and interoperability and also to put in place joint data stewardship programmes aligned with a common understanding.

7.18 The principle of *accountability* requires, as a minimum, transparency in the use and sharing of data in the context of big data and AI use in biomedical research across borders; it also promotes public scrutiny of decision-making processes, which is imperative to maintain public trust across countries. Nonetheless, as countries have

[21] Liverani, M., Teng, S., Le, M. S. *et al*. (2018). Sharing Public Health Data and Information Across Borders: Lessons from Southeast Asia. *Globalisation and Health*, *14*(1), 94. https://doi.org/10.1186/s12992-018-0415-0

[22] Research Data Alliance (RDA). (2021). Navigating Data Sharing in International Research Collaborations. *Research Data Alliance.* Retrieved January 16, 2023. https://www.rd-alliance.org/sites/default/files/iN2N%20October%202021%20Webinar%20slides%20to%20PDF%20-%20FINAL_0.pdf

[23] Lea, N. C., Nicholls, J., Dobbs. *et al*. (2016). Data Safe Havens and Trust: Toward a Common Understanding of Trusted Research Platforms for Governing Secure and Ethical Health Research. *JMIR Medical Informatics, 4*(2), 22. https://doi.org/10.2196/medinform.5571

different interpretations and understanding of transparency and with varying levels of big data and AI technological readiness, having a common commitment and understanding on accountability and the technical processes required to maintain transparency in their big data and AI systems would be crucial. This would allow international research collaborations to be managed in a way that is consistent with associated international standards and norms, and that respects the rights and interests of all relevant stakeholders, including research participants, researchers, and the broader public from various countries.

7.19 The use of a third-party broker has been recommended to maintain cross-border cooperation, mediate linguistic barriers, create a common legal framework, and address ethical issues that may result from the sharing of data across borders.[24] The World Health Organization (WHO) and other global health actors such as the Council for International Organisations of Medical Sciences (CIOMS) have also issued recommendations and guidelines on ethical principles to promote closer links between regional partners. These include *respect for persons,* specifically of those who are capable of deliberation about their personal choices and protection of vulnerable persons of diminished autonomy; *beneficence* to maximise benefits and minimise harm; as well as *justice* in ensuring that no one is unfairly disadvantaged for access to the benefits of big data and AI use in biomedical research. While big data sharing and collaboration between countries promote benefits, there are also significant cross-sectoral challenges arising from big data sharing.[25] Different non-biomedical sectors often involve distinct research cultures, standards, expectations, training and ethics and researchers should consider these aspects in tackling challenges from big data and AI use in biomedical research.

Data Regulatory Frameworks Currently in Place

7.20 Reflecting the focus of this chapter on good governance and responsible use, rather than legalistic notions of data ownership, it is important to note how this also mirrors regulator frameworks. Legislation and guidelines have been implemented by governments of various countries to regulate the collection, storage, and usage of data in biomedical research that focus mainly on the protection of an individual's rights over their personal data, regulation of personal data use by corporations, research institutions, and healthcare institutions, and how data may be consolidated into efficient, secure, and accessible platforms. Some existing practices and frameworks are highlighted and discussed in terms of the ethical principles and technical standards. The General Data Protection Regulations (GDPR)[26] establishes guidelines for the use of personal data while the Findable, Accessible, Interoperable and Reusable (FAIR) Data Principles[27] were developed by the scientific community to allow information to be more accessible. GDPR and FAIR were chosen as these

[24] Bird, E., Fox-Skelly, J., Jenner, N. *et al*. (2020). The Ethics of Artificial Intelligence: Issues and Initiatives. *European Parliament*. Retrieved February 23, 2023. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

[25] Laurie, G. T. (2019). Cross-sectoral big data: The Application of An Ethics Framework for Big Data in Health and Research. *Asian Bioethics Review, 11*(3), 327-339. https://doi.org/10.1007/s41649-019-00093-3

[26] EU General Data Protection Regulation. (2022). *GDPR.eu.* Retrieved November 23, 2022. https://gdpr.eu/tag/gdpr/

[27] Wilkinson, M. D., Dumontier, M., Aalbersberg, I. *et al*. (2016). The FAIR Guiding Principles for Scientific Data Management and Stewardship. *Scientific Data, 3*(1), 160018. https://doi.org/10.1038/sdata.2016.18

two are more prominent international frameworks, and TRUST is a local framework for biomedical research.

Examples of Data Sharing Frameworks

General Data Protection Regulations (GDPR)[26] – European Union

The GDPR addresses the regulation and protection of individuals' control and rights over their own personal data (not specific to research), defined as data that allows a living person to be directly, or indirectly, identified from data that is available. There are also a few special categories of sensitive personal data that are given greater protections. A person's health data falls into the category of sensitive personal data. The GDPR governs all processing of 'personal data' and clearly articulates a full suite of responsibilities for 'data custodians/controllers' and 'data stewards/processors' (see sections 7.1 to 7.7 above).

The GDPR has seven broad principles that are intended to protect the privacy and rights of individuals *(respect for persons)* in relation to their personal data:

a. Lawfulness, fairness, and *transparency*: Personal data must be processed in a way that is lawful, fair, and transparent to the individual.

b. Purpose limitation: Personal data must be collected for specified, explicit, and legitimate purposes, and must not be processed in a way that is incompatible with those purposes.

c. Data minimisation: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

d. Accuracy: Personal data must be accurate and, where necessary, kept up to date.

e. Storage limitation: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

f. *Integrity* and confidentiality: Personal data must be processed in a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

g. *Accountability*: The custodian/controller (the person or organisation that determines the purposes and means of processing personal data) must be responsible for, and must be able to demonstrate compliance with the GDPR principles via proper documentation.

These principles act as an overarching framework that is designed to lay out the broad purposes of GDPR. GDPR places the greatest responsibility on data custodians and stewards, as it was designed to protect the rights of individuals. Under the GDPR, 'data controllers/processors' are adopted as legal terms with specific assigned responsibilities whereas in this report, we use 'data custodians/stewards' to define the ethical roles that broadly mirror these legal categories.

PDPC's Advisory Guidelines for the Healthcare Sector (2017)[14] - Singapore

The guidelines were developed jointly by Singapore's MOH and PDPC to address the unique circumstances faced by the healthcare sector in complying with the PDPA 2012. PDPA provides a baseline standard of protection for personal data in Singapore. PDPA comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore. PDPA also provides the establishment of a national Do Not call Registry, where individuals may register their Singapore contact number with, to opt out from receiving unwanted telemarketing messages from organisations. Through the development of a set of sector specific guidelines for healthcare, it guides healthcare licensees and professionals to apply a baseline and uniformed standard of healthcare data protection for all patients' health data.

The guidelines consist of two main parts:

- The first part covers the application of PDPC's data protection provision to the healthcare sector.
- The second part covers the application of PDPC's Do Not Call provisions to the healthcare sector.

FAIR (Findable, Accessible, Interoperable and Reusable) Data Principles[27]

The FAIR Data Principles (**F**indable, Accessible, Interoperable, and Reusable) are a set of guiding principles proposed by a consortium of scientists and organisations to make scientific data (including medical and research data) findable, accessible, interoperable, and reusable. The FAIR Data Principles were developed in response to the increasing importance of data in research and the need to ensure that data is properly managed, preserved, and shared. These principles have since been adopted by research institutions worldwide, and are based on the following key objectives:

a. Findable: Data must be easy to locate and identify, using persistent identifiers and machine-readable metadata.

b. Accessible: Data must be easily accessed and retrieved, using open and standard protocols, licences, and application programme interfaces.

c. Interoperable: Data must be able to be connected and integrated with other data sources, using open and standard data formats and vocabularies.

d. Reusable: Data must be able to be used and re-used by different users and systems, in a way that is ethical, transparent, and reproducible.

The FAIR Principles are a set of best practice guidelines for the preparation of data for sharing. FAIR data enables computational systems to find, access, interoperate, and reuse data with no or minimal human intervention. The FAIR Data Principles also provide a data management framework to help researchers manage their data assets whilst addressing the ethical considerations such as protection of privacy and confidentiality of research participants and ensuring respects for persons through informed consent taking.

Additionally, by sharing data that are FAIR, researchers facilitate knowledge discovery and increase the chance of possible collaboration, which are beneficial especially for early-career researchers.

TRUST Platform[28] – Singapore

TRUST is a local data exchange platform that aims to bring together large-scale datasets to address important health-related questions, such as patient health conditions, development of new medical treatments, planning of health programmes and enhancement of public health policies, that cannot be tackled by individual research institutions or public sector agencies. Data contributors include public health institutions, research institutions, and public agencies that allow their anonymised data to be made accessible via TRUST for research analysis. Data requestors or users include healthcare professionals, researchers, and academics who use the data made available on TRUST for research. TRUST aims to standardise data access security protocols across multiple sources through consolidation into a single platform, reduce data access time, and store and process data in an 'accessible, interoperable and trusted manner'.

The TRUST Platform is focused on four key areas:

a. Encourage responsible practices in the use of data and technology, and promote the development and adoption of ethical guidelines and best practices to ensure that the rights and interests of all relevant stakeholders are taken into account.

b. Engage with policymakers and regulators to promote the development of effective and appropriate policies and regulations for the use of data and technology to ensure that the use of data and technology is consistent with relevant laws and regulations, and protects the privacy and rights of individuals.

c. Promote capacity and awareness among stakeholders about the responsible use of data and technology to ensure that stakeholders use data and technology in an ethical and responsible manner.

d. Foster open and transparent dialogue among stakeholders to discuss, share, and collaborate on issues related to the responsible use of data and technology to promote trust and understanding among stakeholders, to address ethical concerns and challenges related to the use of data and technology.

[28] TRUST (2023). Improving Health Outcomes Through Trusted Data Exchange. *MOH TRUST*. Retrieved January 16, 2023. https://trustplatform.sg/

CHAPTER 8: DATA PRIVACY, ACCESSIBILITY AND SECURITY

This chapter discusses the concepts and inter-relationship of data privacy, accessibility and security and the ethical considerations in maintaining data privacy and enhancing data security and accessibility in the use of big data and AI in biomedical research.

Data Privacy

8.1 Data privacy encompasses patient confidentiality and concerns how data, including sensitive, personal data, should be collected, stored, managed, used, and shared with any third parties, in accordance with data subjects' preference, consent or control over their own data. Data privacy enables individuals to decide and limit access to the use or sharing of their personal data. A key pillar of data privacy is ensuring compliance with applicable data protection laws and regulations and the law relating to confidentiality.[1] Many traditional data protection frameworks are inadequate in handling the volume, variety, and velocity of large and complex data sets, as explained further below. Breaches in data privacy pose major risks for biomedical research and public trust, particularly when using substantial amounts of personal or individual information. For all these reasons, robust and dynamic privacy protection regimes are required to promote scientifically sound and ethically robust research, while protecting against misuse of ever-expanding datasets.

Data Accessibility

8.2 Data accessibility refers to the extent to which third parties can access and retrieve data stored within a database or other repository.[2] Easily accessible data is vital to enable bona fide third parties to quickly extract relevant information to make informed or educated decisions in biomedical research. Robust data accessibility requires sound governance regimes to control and monitor access, placing data subjects' rights at the forefront of all access requests. Assuming such regimes are in place, and leaving aside security concerns, there is an imperative for data to be used in ways that fully respect persons and with minimal barriers so that it can be leveraged to its fullest. Respecting individuals' autonomy often entails the seeking of consent, but this is not always possible or practicable, as discussed elsewhere in the report. Nonetheless, data in human biomedical research is heterogeneous and often derived from various sources; this can limit data accessibility and pose a challenge for researchers to effectively probe and utilise data. This in turn hampers the development of technologies in big data.

Data Security

8.3 Data security entails technical practices, processes and measures put in place to ensure that personal data is protected from unauthorised access, data corruption or theft by third parties, including internal and external hackers.[3] Data security includes

[1] Storage Networking Industry Association (SNIA). (2022). What Is Data Privacy? *Storage Networking Industry Association (SNIA).* Retrieved January 3, 2023. https://www.snia.org/education/what-is-data-privacy

[2] Sridharan, M. (2022). Data Accessibility. *Think Insights.* (2022, June 2). Retrieved January 3, 2023. https://thinkinsights.net/data-literacy/data-accessibility

[3] Sharon, S. (2022). What Is Data Security? The Ultimate Guide. *TechTarget.* (2022, Aug 11). Retrieved January 3, 2023. https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know

the areas of encryption, authentication, quality assurance, access control, threat monitoring, breach access and recovery, as well as prevention of data loss. Maintaining data security is a priority for healthcare organisations and research institutions. Singapore's Personal Data Protection Commission (PDPC) and the Ministry of Health developed the Advisory Guidelines for the Healthcare Sector[4] in 2014. The guidelines set out and elaborate on the PDPC's interpretation of enforcement of provisions relating to data protection under the Personal Data Protection Act (PDPA) 2012. These guidelines assist organisations and individuals' understanding of the PDPA. Most recently, the guidelines were revised in 2017 to address the unique circumstances (e.g., medical data has a larger amount of sensitive information as compared to personal data) faced by the healthcare and biomedical research sector in complying with the PDPA 2012. In the US, medical organisations and their staff are required to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule when handling protected health information.[5] The HIPAA Security Rule provides guidelines for health service providers regarding storing, transmission, authentication protocols, and controls over access, integrity, and auditing. Similar frameworks for healthcare data security have also been developed in Australia,[6] Canada,[7] the UK,[8] as well as other countries and regions, such as in Europe through the General Data Protection Regulation (GDPR).

Inter-relationship Between Data Privacy, Accessibility and Security

8.4 Biomedical researchers often need to assimilate and analyse copious amounts of research, clinical and personal data. This necessitates the development of national guidelines on safe data use and infrastructure (e.g., databases or repositories subject to robust governance regimes) for secure data storage to deliver adequate privacy protection and security of the data relating to individuals. *Data privacy* requires the responsible governance and use of data to avoid compromising individuals' personal data rights and interests, while *data security* is concerned with technical security systems put in place to protect individual data from malicious threats or unsafe uses and to limit and control data access to only authorised personnel. Such regimes work together to prevent data loss and misuse through unauthorised access and promotes privacy and the protection of the identity of participants. At the same time, however, care must be taken to promote responsible data accessibility, i.e., ease of access to

[4] Advisory Guidelines for the Healthcare Sector (2017 Revised Edition). *Personal Data Protection Commission.* Retrieved January 5, 2023. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf

[5] Office for Civil Rights. (2022). Summary of the HIPAA Security Rule. *U.S. Department of Health and Human Services* (*HHS).* (2022, October 19). Retrieved January 3, 2023. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[6] The Office of the Australian Information Commissioner. (2023). Guide to Health Privacy. *The Office of the Australian Information Commissioner*. (2023, March 10). Retrieved April 18, 2023. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/guide-to-health-privacy

[7] Office of the Privacy Commissioner of Canada. (2017). Who to Contact with Concerns About the Protection of Your Personal Health Information. *Office of the Privacy Commissioner of Canada*. (2017, February 21). Retrieved March 6, 2023. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/02_05_d_70_phi/

[8] National Health System Digital UK. (2022). Protecting Patient Data. *National Health System Digital UK*. (2022, November 14). Retrieved March 6, 2023. https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/protecting-patient-data

the repository to legitimate third parties. Privacy protection is not an absolute; good governance is about finding and maintaining the delicate balance between robust privacy protection and granting access in the public interest to trustworthy parties who seek it.

Issue 1 – How do we ensure robust data security and proper access control while also maintaining data privacy in the use of big data and AI in biomedical research?

8.5 Control of data access is a key consideration for ensuring data privacy, even for anonymised data. Authorities, institutions, and parties may be allowed access only when necessary to facilitate relevant research projects. The respective responsibilities of institutions and parties who have been granted access to the data to ensure and maintain data privacy on an ongoing basis remain. Several possible methods to control data access include the following:

a. Blockchain technologies enable security systems deployed in organisations to use distributed key public infrastructure to authenticate devices and uses, and may be employed to prevent data theft, fraud, identity theft and other forms of cybercrime. This is possible because these technologies control how data is accessed and shared.[9] A blockchain-based big data solution, involves a decentralised secure tracking system for any data interactions that could occur in research, and allows the sharing of data with authorised parties, through using cryptographic algorithms (e.g., an encryption algorithm and an encryption key), where only authorised parties can encrypt and access particular data during interactions, protecting the security of sensitive data and reducing risks (e.g., security attacks, data leakage, data tampering, etc.). This platform not only enhances data sharing, increases openness and transparency and accountability, but also has leading-edge advantages in protecting data confidentiality, integrity, and availability. For instance, the data encryption and cryptography mechanisms prevent the data from being tampered with and forged; and the complex checksum sharing mechanism ensures data integrity, availability, and confidentiality. Such technologies allow individuals to easily control and share their personal data while maintaining their privacy and also enable researchers to securely access information for biomedical research purposes.[10]

b. Commercial platforms may facilitate data access to biomedical and clinical data for AI research. For example, IBM's Watson Health is an AI platform that shares and analyses health and clinical data among hospitals, providers, and researchers.[11] However, the role of third parties in the biomedical research in ensuring that data privacy is not compromised would have to be examined and

[9] Frank, R. & Dr Robert S. (2019). Healthcare 2019: The Year of the Big Data Blockchain. *HealthManagement 19*(1). Retrieved January 3, 2023. https://healthmanagement.org/c/hospital/issuearticle/healthcare-2019-the-year-of-the-big-data-blockchain

[10] Zhang, W., Qamar, F., Abdali, T.-A.N. *et al.* (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics, 12*(3), 546. https://doi.org/10.3390/electronics12030546

[11] Chen, Y., Argentinis, E. J. D. & Weber, G. (2016). IBM Watson: How Cognitive Computing Can Be Applied to Big Data Challenges in Life Sciences Research. *Clinical Therapeutics, 38*(4), 688–701. https://doi.org/10.1016/j.clinthera.2015.12.001

managed through formal agreements, established operating procedures and secure data platforms. An example is the 'Data Safe Haven', which is a secure data platform that provides a safe environment supported by trained staff and agreed processes whereby data can be processed and linked with other health data and made available in a de-identified form for analysis to facilitate research. 'Safe Havens' accords users (e.g., researchers and third parties) access based on user accreditation and compliance with high standards of data security.[12] It is a safeguard for confidential data being used for research purposes as any researchers or third parties applying for access to the data must adhere to the 'Safe Havens' principles.

8.6 In addition, institutions should place emphasis on data governance to deploy proper mechanisms to protect data privacy. Institutions should control access to data through user roles, use purposes and consent obtained from individuals for data use, where consent is appropriate. Institutions should also set out the responsibilities of parties that access the data and put in place mechanisms to manage any breaches. Routine audits (i.e., security audits) on the technological environments used by the institutions to perform data access and manipulation would identify system issues or other security vulnerabilities and in turn, enhance data security.

8.7 In balancing the objective of promoting data accessibility with the imperative of adequately protecting data privacy, some key ethical principles including *respect for persons*, *solidarity* and *proportionality* should be considered:

a. The principle of *respect for persons* requires the importance for institutions to respect the privacy of citizens whose data is used and participants who have agreed to take part in research.

b. The principle of *solidarity* requires that researchers balance personal data protection (individuals' interests and needs) with that of furthering biomedical AI research which relies heavily on vast amounts of personal data to achieve high predictive performance (collective interests and needs).[13]

c. The principle of *proportionality* requires that when ensuring data privacy, researchers are cognisant of competing interests at hand, i.e., data accessibility and security, and vice versa. *Proportionality* requires that the regulation and governance of data accessibility and security are appropriate individually and collectively, in relation to the research intent while ensuring adequate individual data privacy. The anticipated risks and extent of regulation and governance should not be disproportionate to any anticipated benefits nor to the adequate protection of citizens' rights.

[12] Lea, N. C., Nicholls, J., Dobbs, C. *et al*. (2016). Data Safe Havens and Trust: Toward a Common Understanding of Trusted Research Platforms for Governing Secure and Ethical Health Research. *JMIR Medical Informatics, 4*(2), e22. https://doi.org/10.2196/medinform.5571

[13] Prainsack, B., & Buyx, A. (2012). Solidarity in Contemporary Bioethics - Towards a New Approach. *Bioethics, 26*(7), 343–350. https://doi.org/10.1111/j.1467-8519.2012.01987.x

Issue 2 – How can institutions or parties accessing and using the data ensure data privacy?

8.8 Research institutions and researchers conducting studies involving humans and their data are obliged to protect the privacy of their citizens. This duty entails that safeguards and measures to protect the data privacy of the participants are put in place throughout all stages of the research cycle, including recruitment (where this occurs as an active practice, as opposed to accessing existing datasets); initial collection of data; use and analysis of data; dissemination of findings; storage and retention of data; and disposal of records. Organisations should know what the data collected is and used for, how it will be protected and that it should be retained only for as long as it is needed.

8.9 The specific type of safeguards and protective measures[14] to be introduced depends on the type of research projects that are carried out, and local laws on data protection, confidentiality, and privacy (broadly defined). As a general rule, safeguards may be categorised into:

a. *Physical safeguards* that refer to the securing of physical locations storing research participants' data from access by unauthorised personnel;

b. *Administrative safeguards* that distinguish between those with access to data from those without;

c. *Technical safeguards* that include digital locks that protect the personal data of individuals; and

d. *Research design safeguards* that protect the privacy of study participants by established operating procedures.

8.10 In deliberating the choice(s) of safeguards and measures to protect data privacy, the following ethical principles should be considered:

a. The principle of *respect for persons* requires that the welfare and interests of individuals are protected, including the privacy and confidentiality of their data used in biomedical research. Where appropriate, *respect for persons* might also be demonstrated by seeking consent to data use, but this is not always possible for all kinds of research.

b. *Accountability* ensures that research participants are informed, where practicably possible, by researchers and/or their institutions of how and for what purposes their data will be used, as well as the parties who will be accessing their data. Researchers and research institutions are responsible in ensuring that safeguards which are put in place work effectively.

[14] Kruse, C. S., Smith, B., Vanderlinden, H. *et al*. (2017). Security Techniques for the Electronic Health Records. *Journal of Medical Systems, 41*(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Issue 3 – How can institutions/organisations/parties managing data stored in multiple on-site servers or cloud repositories ensure appropriate data accessibility?

8.11 With increasing use of big data and AI in biomedical research, institutions and organisations often face challenges in the management of data storage, particularly in genome sequencing research where large volumes of genetic data are generated. Many institutions and organisations store data in their own premises due to the advantages of control over security, access, and uptime.[15] However, an on-site server network containing stored data should be managed carefully to enable access to parties for beneficial outcomes, without compromising data security and data privacy. With decreasing costs and increasing reliability, cloud-based storage is emerging as an alternative option that some healthcare organisations have opted for to enhance data accessibility and use. Despite the advantages, there are potential concerns that cloud-based storage might increase the risk of cybersecurity attacks and unauthorised access to data distributed and stored at multiple locations. Therefore, institutions and organisations must choose cloud-based storage partners that understand the importance of healthcare-specific compliance guidelines, and other ethical and security issues to store data and regulate access to parties.

8.12 In managing stored data, the principle of *proportionality* should be considered by research institutions and organisations to ensure that the degree or extent of restricting access to the relevant parties, or imposing conditions on their access, is appropriate to meet the research intent and proportionate to potential benefits to the research participants and society.

8.13 An example of a data framework developed to deliver data security and data accessibility while ensuring data privacy in biomedical research is Singapore's 'TRUST platform', established in 2022. The 'TRUST platform' serves as a consolidated national health-related data exchange platform that allows public health institutions, research institutions, public agencies, and private sectors to contribute and use data for research. Various types of data are collected and stored in the platform including health-related, behavioural, and socio-economic data. The TRUST platform's data governance policy sets out stringent data sharing conditions and restricts data access to TRUST members whose request meet the research intent and is proportionate to potential benefits to the research participants and society, adhering to the ethical principles of *proportionality, accountability,* and *solidarity*.[16] Key aspects of the TRUST platform that enable good data governance include:[17]

a. Secure access to health-related research and real-world data through appropriate cybersecurity safeguards;

[15] National Academy of Sciences, National Academy of Engineering, Institute of Medicine, Committee on Science, Engineering, and Public Policy. (2009). Ensuring Access to Research Data. *Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age*, Chapter 3. National Academies Press. https://www.ncbi.nlm.nih.gov/books/NBK215271

[16] TRUST. (2023). General Information about Research on TRUST. *TRUST Platform.* Retrieved January 3, 2023. https://trustplatform.sg/faqs/general-information-about-research-on-trust/

[17] TRUST. (2023). TRUST Vision and Mission. *TRUST Platform.* Retrieved January 3, 2023. https://trustplatform.sg/about-us/what-is-trust-2/

b. Data accessibility and sharing enhanced through interoperability of systems (e.g., large volumes of interoperable curated datasets shared securely);

c. Restricted data access where researchers registered as TRUST members, must submit a data request before being allowed to access TRUST data. The scientific, clinical, and health value of such requests will be reviewed by the Data Access Committee[18] to determine if the purpose of data use is beneficial to the public and can generate social benefit and is in line with the TRUST's data governance protocols; and

8.14 Institutions/organisations/parties should adhere to TRUST's data governance framework, policies, and protocols, particularly with respect to complying with the data sharing conditions set out for the use of big data in biomedical research.

Issue 4 – How should institutions manage big data heterogeneity found in AI model construction methodologies?

8.15 As large amounts of data and computer resource are required to construct powerful AI models based on large or complex (even billion-scale) networks, researchers have developed the machine learning methodologies[19] to avoid starting afresh, and instead build accurate models on top of existing models. Through this methodology, developers can leverage on existing models developed by Google, OpenAI and Meta to build high performing models instead of starting from scratch. As such, it is common practice to import and utilise pre-trained networks built on datasets collected from the world wide web. Examples include Bidirectional Encoder Representations from Transformers (BERT), a machine-learning technique for natural language processing, and Generative Pre-trained Transformer 4 (GPT4), which is a deep learning model that generates text from data available on the internet. While pre-training has documented benefits in improving model performance, it is important to note that it could also be a source of vulnerability for resulting AI models.

8.16 The datasets used to construct AI methods have typically been based on the world wide web and managed by big technology companies like Google, Open AI, Meta and the open-source community. Malicious attacks on databases and code bases of pre-trained models are of concern if new AI models use them blindly as the basis for transfer learning, and inadvertently inherit these vulnerabilities. Therefore, a good starting point for safe sharing and use of data and models would be controlled data and model sharing.[20] This comprises:

[18] Members of the Data Access Committee are individuals with the requisite domain knowledge in healthcare, science, technology, law, ethics and senior representatives from TRUST partner institutions. Retrieved January 5, 2023. https://trustplatform.sg/about-us/governance/

[19] Niklas D. (2022). What Is Transfer Learning? Exploring the Popular Deep Learning Approach. *Built In.* (2022, August 25). Retrieved January 3, 2023. https://builtin.com/data-science/transfer-learning

[20] Model Artificial Intelligence Governance Framework. (2022 Second Edition). *Personal Data Protection Commission*. https://www.pdpc.gov.sg/help-and-resources/2020/01/second-edition-of-model-artificial-intelligence-governance-framework

a. *Data sovereignty* which is the ability of an individual or organisation to be completely independent from other individuals or organisation with regard to management and control of data;

b. *Trust* between parties that can be promoted through proper verification of authorised individuals involved in the biomedical research, and authentication of external big data sources' and AI models' legitimacy; and

c. *Security systems and measures* put in place to warrant that data shared is protected against unauthorised use, whether malicious or accidental, and that storage, transport and software are adequate.

8.17 Researchers should also adhere to the ethical principles of *integrity*, *transparency,* and *accountability* to demonstrate that there is transparency in the design and use of pre-trained models, and the pre-trained models selected are reliable and appropriate. The importance of this cannot be overstated, given that these models may be used to analyse data for decision-making, such as use of AI in predictive modelling; the application of big data to identify patterns and anticipate future trends in biomedical research and facilitate the development of medical treatments that benefit individuals and society.

CHAPTER 9: ANONYMISATION, DE- AND RE-IDENTIFICATION OF DATA

This chapter discusses the concepts of data anonymisation, de- and re-identification of data, and their value in big data and AI research. The ethical considerations of data anonymisation, de- and re-identification of data in the use of big data and AI in biomedical research are also discussed here.

Data Anonymisation

9.1 Data anonymisation refers to the process of preserving private or sensitive information by removing identifiers that connect an individual to the stored data.[1] Technical safeguards are put in place to reduce the risks of identification significantly, which protect individual's privacy and help organisations using personal information such as patient data, adhere to strict data privacy regulations.[2] A method commonly used in data anonymisation is k-anonymity where a higher k value is associated with a lower probability of re-identification.[3]

Data De- and Re-identification

9.2 Data de-identification entails removal of personally identifiable information to protect privacy.[160] However, de-identified data may not necessarily be anonymised data, as there is a possibility to re-associate the data with the individual at a later time via aggregated information e.g., code, algorithm, or pseudonym. In some cases, the de-identified data may need to be re-identified to track the activity of an individual in the data set.

9.3 Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in the US, data related to health may be considered de-identified when specified data elements such as names, street address, ZIP code, dates directly related to an individual (e.g., date of birth), mobile, fax, IP addresses and identifiers, etc., are removed.[160] Similarly, in Australia, the Office of the Australian Information Commissioner (OAIC) recommends that the first step of data de-identification should involve the removal of direct identifiers such as name or address, before removing or altering other information that allows re-identification, and/or use controls and safeguards in the data access environment to manage the risk of re-identification.[4]

9.4 While anonymised data can be considered as a particular subset of de-identified data, it may not always be in the best interest of the individual or institution to seek anonymisation of data, as there may be a legitimate need to trace back to the user or individual under certain scenarios. These may include contacting people regarding

[1] Guidelines for Data De-Identification or Anonymisation. (2015 edition). *EDUCAUSE.* https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/guidelines-for-data-deidentification-or-anonymization

[2] Corporate Finance Institute. (2022). Data Anonymisation. *Corporate Finance Institute.* Retrieved December 25, 2022. https://corporatefinanceinstitute.com/resources/business-intelligence/data-anonymization/

[3] El Emam, K., & Dankar, F. K. (2008). Protecting privacy using k-anonymity. *Journal of the American Medical Informatics Association (JAMIA), 15*(5), 627–637. https://doi.org/10.1197/jamia.M2716

[4] De-identification and the Privacy Act 2014 (2018 Revised Edition). *Office of the Australian Information Commissioner.* https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act#what-does-a-de-identification-process-involve

their risk of disease and extraction of meaningful clinical survey results. Data re-identification to identify a person can also be achieved by recombining de-identified datasets and publicly available or auxiliary information. The risk of re-identification depends on the identifiable external data sources which are available to the public. Medical data such as computerised axial tomography (CAT) scans or magnetic resonance imaging (MRI) with which a person's face can be reconstructed from combination of several results are prone to re-identification. This is true even after identifying information such as gender, sex, age, and identification number have been removed, given that it is becoming increasingly easy to identify a person by using certain types of health data.

Data Risk Management

9.5 As the risk of data re-identification increases with 'identifiable data' found in many biomedical research and clinical practices, data risk management becomes a crucial process to mitigate the risks. Data risk management is a process where researchers and organisations follow when they acquire, store, process, transform, and use data to manage and reduce data risks.[5] Data risks often arise as a result of poor data governance, data mismanagement and poor data security. When data is at risk, there are costs incurred such as repairing the damage to IT infrastructure, regulatory fines and time spent to contain an incident. Having a risk management process that starts with identifying the potential threats and risks, conducting a risk assessment to find out the nature and likelihood of damage from a specific risk, followed by a risk response where new controls are added or avoiding actions that might trigger the risk and putting in a risk monitoring process to monitor and report risks, will reduce the risks from data re-identification.

9.6 Anonymisation, de- and re-identification of data as well as data risk management are often applied in biomedical research and are important concepts and tools to enable data to be used, analysed, and managed in safe and secure ways that promote responsible data use while protecting individual privacy and interests.

Issue 1 – Are current methods of de-identification and anonymisation still applicable when large volumes of personal, health and medical data are used in big data and AI research?

9.7 The Personal Data Protection Commission (PDPC), which administers the Personal Data Protection Act (PDPA) 2012 in Singapore, describes 'de-identification' as either a reversible or irreversible process of modifying personal data into information that cannot be used to identify individuals.[6] In biomedical research, analyses involving big data and AI algorithms rely increasingly on large volumes of personal, health and medical data. The PDPC recommends that organisations engage data anonymisation experts, statisticians, or independent risk assessors to evaluate and facilitate appropriate anonymisation techniques employed, particularly for large

[5] Tobias G.M (2019). What Is Data Risk Management? *datto*. Retrieved February 25, 2023. https://www.datto.com/blog/what-is-data-risk-management

[6] Advisory Guidelines on the Personal Data Protection Act for Selected Topics 2013 (2022 Revised Edition). *Personal Data Protection Commission.* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.pdf

complex datasets.[165] Research institutions may also put in place other controls such as:

a. limiting the number of people to whom the information is available and accessible;

b. imposing restrictions on the users of the data and subsequent (if any) linkage or disclosure of the data;

c. requiring users of the data to implement processes to ensure appropriate use of de-identified data;

d. requiring users of the data to take adequate steps to remove and completely erase data after use for biomedical research; and

e. limiting the access of users of the data to information that could enable re-identification of de-identified data. This can be achieved through organisational policies and agreements, administrative rules, technical measures such as encryption to restrict access to the information, limiting access to only authorised users, controlling access through passwords, and other physical measures to restrict access to information storage areas.

9.8 Nonetheless, conventional methods of de-identification and anonymisation, when applied to large-scale cohort research and real-world personal, health and medical data, may face limitations and challenges in their roll out. One challenge is whether a common consensus could be reached on the clear definitions and fundamental concepts of de-identification and anonymisation within the research community.[7] Both terms have been used with discrepancies by researchers which has led to difficulty in standardising procedures. Some researchers chose to hide or remove identifiers while others replace them with pseudonyms. Although there may not be universal definitions or adoption of the aforementioned terms at present, researchers of specific studies should adhere to the ethical principle of *consistency* to ensure similar or interoperable standards are applied in their research protocols to standardise processes. This includes specifying the definitions used in the biomedical research and/or making references to definitions and guidance provided in major legislations on personal data protection, such as the General Data Protection Regulations (GDPR), HIPAA and PDPC where appropriate.[166]

9.9 De-identifying and anonymising (especially textual) data is also time-consuming, depending on the complexity and type of data. For instance, structured data is easier to process than unstructured data; specific types of information, such as diagnoses of rare diseases and large genome sequence data, may be more sensitive by nature and may carry a higher risk of breach of the confidentiality of the participants' identities. Therefore, researchers may face difficulties in overcoming the interdependence between data quality assurance and identifiability in their work, since the privacy of research participants may be inadvertently compromised. Researchers should, to the best of their abilities, consider the following ethical

[7] Chevrier, R., Foufi, V., Gaudet-Blavignac. *et al.* (2019). Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review. *J Med Internet Res, 21(5), e13484. https://doi.org/10.2196/13484*

principles when employing de-identification and anonymisation to big data use in biomedical research:

a. The principle of *respect* for persons requires that the welfare and interests of individuals are protected, including their privacy and confidentiality of their data used in biomedical research (See Chapter 8: Data Privacy, Accessibility and Security); and

b. The principle of *proportionality* requires that researchers achieve an appropriate balance between data quality assurance and identifiability of data, in relation to the research intent and its anticipated benefits and risks. The risk of re-identification of anonymised data increases with the addition of new data to existing large datasets and re-identification then becomes possible through data linkage techniques.[166] Hence, the ethical principle of *proportionality* should be considered with the use of data use agreements, de-identification and anonymisation processes, to mitigate this risk.[166]

9.10 Institutions have also expressed concerns about the cost[8] and diverse data sources, particularly for investigators who would require data sharing in collaborative biomedical research projects. Transnational differences in anonymisation and de-identification systems and processes among countries and the need for natural language processing systems to process varied languages compound the issue. Absence of practical guidelines and training for researchers has been highlighted as an additional concern.[9] Nevertheless, while anonymisation may not be entirely possible with handling large volumes of data and may not be easily achievable with existing AI methods, institutions should take steps to de-identify or reduce the risk of re-identification of confidential patient data, in line with the principle of *proportionality*.

Example of an initiative (work in progress) to manage responsible data usage: Singapore's On-Premise Research Data Science and Systems Explorer (ODySSEy) Platform[10]

ODySSEy is a programme currently in development by SingHealth and Duke-NUS which contains data from the SingHealth electronic data warehouse and carries approved identifiable and de-identified data for research projects. It is built for research and decoupled from clinical operations, and provides a secure, efficient, and reliable access to data under the Human Biomedical Research Act (HBRA) regime. The ODySSEy Platform is able to preserve institutional integrity and patient privacy under the HBRA and aims to provide researchers access to a mix of identifiable and anonymised health data, tailored for research purposes while at the same time protects

[8] The Wall Street Journal. (2022). 3 Data Management Challenges and 4 Ways to Respond. *The Wall Street Journal.* Retrieved December 25, 2022. *https://deloitte.wsj.com/articles/3-data-management-challengesand-4-ways-to-respond-01666114130*

[9] Choi HJ, Lee MJ, Choi C. *et al*. (2015). Establishing the role of honest broker: Bridging the gap between protecting personal health data and clinical research efficiency. *PeerJ, 3*, e1506, https://doi.org/10.7717/peerj.1506

[10] SingHealth Duke-NUS Academic Medical Centre. (2022). ODySSEY Platform. *SingHealth Duke-NUS Academic Medical Centre.* Retrieved December 25, 2022, https://www.singhealthdukenus.com.sg/research/hsrc/Pages/odyssey-platform.aspx

patient or research participant's privacy through the regulation of data access via HBRA frameworks.

Issue 2 – How can the risks of re-identification be managed when linking data from multiple sources?

9.11 Big data and AI research have vast potential but are often accompanied by corresponding risks, including (but not limited to) high risks of re-identification of data subjects. The Common Rule Agencies, a collection of multiple US federal agencies and departments including the US Department of Health and Human Services, acknowledged that re-identification is becoming gradually easier because of 'big data' – which they define as (?) the abundance and constant collection and analysis of information with the evolution of technologies and the advances of algorithms.[11]

9.12 With greater volume and variety of data in big data and AI use in biomedical research, it is increasingly difficult to sufficiently de-identify a data set while retaining the integrity of the data for analysis. As a result, it is possible for individuals to decrypt ostensibly de-identified data (cryptographic attacks) or re-identify individuals in a dataset by matching the data with other (identifying) datasets (linkage attacks) with relative ease.[12]

9.13 In Singapore, unauthorised re-identification of anonymised information is an offence under Part 9B of the PDPA. The PDPC advises that when assessing the risks of data re-identification, organisations should review whether the data is reasonably de-identified and consider the types of information that could enable re-identification if combined with the de-identified data, as well as the ease with which such information can be accessed. If data cannot be de-identified further due to the need to preserve its granularity, organisations should implement more stringent safeguards including practising data minimisation (i.e., sharing only minimally necessary data attributes, instead of full databases); ensuring data is not disclosed to unauthorised parties; mitigating re-identification risks (e.g., tracking the lineage of data, namely its movement, transformation and usage) and disposing of data properly and promptly after its use.[165] In some cases where the researcher or user becomes the data controller of the de-identified/anonymised data received, he/she should consider the ethical principle of *respect* for persons and ensure that the welfare and interests of individuals are protected, including their privacy and confidentiality of data used in biomedical research. The researcher must uphold high standards of professional and moral conduct when handling the data, and minimise re-identification risks, where possible.

9.14 Under HIPAA, de-identified datasets that do not contain direct or known indirect identifying elements are presumed to be of very low risk of re-identification.

[11] Scholarly Community Encyclopaedia. (2022). Data Re-identification. *Scholarly Community Encyclopaedia. Retrieved January 13, 2023.* https://encyclopedia.pub/entry/32054

[12] Health Legal. (2018). Big Data and the Risk of Re-Identification. *Health Legal. Retrieved January 13, 2023.* https://healthlegal.com.au/current-news/big-data-and-the-risk-of-re-identification/

Nonetheless, HIPAA requires that sharing of such data must be confined by a formal data use agreement or by technical restrictions to avoid or reduce re-identification.[13]

9.15 AI models could also potentially re-identify unique features of an individual's profile from de-identified data fed into algorithms. Ethical use and analysis of complex unstructured data from varied sources have become increasingly difficult as sensitive information may be inadvertently revealed.[14] If security precautionary measures are not sufficient, non-sensitive marketing, health, and financial data may be used by scammers to create false identities. Therefore, the risk of re-identification should be carefully evaluated, and rigorous safeguards put in place prior to the use of AI models. Anonymisation or de-identification of data should be carried out on data from single sources wherever possible to lower the risks of re-identification. The onus is on researchers-users-developers engaging the use of smart systems to implement and abide by guidelines for appropriate use of AI in sorting of complex data to preserve privacy of patients and avoid the risk of re-identification that could lead to potential biases or intrude on an individual's privacy.

9.16 Notwithstanding the type(s) of method employed to minimise data re-identification in big data and AI research, researchers should consider the ethical principles of *respect for persons* and *accountability* to safeguard the privacy and confidentiality of research participants' data and inform research participants of how their data is used and accessed, and ensure that sufficient safeguards and mechanisms are in place to minimise the risk of unwanted or unwarranted re-identification.

9.17 Researchers may also consider other ethical principles such as *solidarity* and *proportionality*. A solidarity-based data governance could be considered to strengthen collective control and ownership of data so that the benefits and costs are borne collectively and fairly. For instance, a remedy for data privacy and protection is to enact effective data obfuscation regulations such as encryption, tokenisation and data masking. Using de-identification, anonymisation and appropriate data classification, big data sets may be used to train AI models without sacrificing the privacy of individuals. Encryption schemes which preserve privacy could be used to run prediction algorithms on encrypted data.

9.18 When assessing the quality of personal data for biomedical research, the principle of *proportionality* requires that only personal data which is adequate (i.e., data robustness and quality) and relevant for the purposes of the study is collected and processed. For fully anonymised or securely de-identified data, appropriate data classification can be used to determine the appropriate handling and storage of the data. This may include data encryption and controlling user access to the data. Data may be disclosed to researchers based on a legal data sharing agreement. Researchers should delete identifiable information as soon as possible after collection.

[13] Simon, G.E., Shortreed, S.M., Coley, R.Y. *et al.* (2019). Assessing and Minimising Re-identification Risk in Research Data Derived from Health Care Records. *eGEMs (Generating Evidence & Methods to improve patient outcomes)*, *7*(1), p.6. http://doi.org/10.5334/egems.270

[14] Cheatham, B., Javanmardian, K. & Samandari, H. (2019). Confronting the Risks of Artificial Intelligence. *McKinsey & Company*. Retrieved December 25, 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence

Issue 3 – Should genetic data be considered exceptional and treated differently from other types of personal and health data?

9.19 Precision medicine, which considers individual variations in genetics, environmental and lifestyle factors, has shown the potential to increasingly transform healthcare at different points of the care pathway and to play a significant role in improving health outcomes. For example, precision medicine better tailors personalised advice and treatment to individuals based on their disease risk, prognosis, and/or likely treatment response to yield greater care benefit; reduces burdens of late-stage chronic disease through targeted prevention and health promotion; avoids complications in individuals at risk of serious adverse reactions; and accelerates definitive diagnosis of patients with rare, serious genetic diseases, thereby reducing diagnostic testing and treatment costs. As such, demands for genomic databanks have surged to meet these research needs. While large volumes of genetic data are necessary for the advancement of genetic sequencing technology, it is imperative to ensure that appropriate security measures and safeguards are in place to protect the informational privacy of contributors. This is particularly so for genetic data which is considered as one of the most sensitive forms of personal data. Genetic data contains unique information of an individual, such as ancestry and health-relevant information (e.g., genetic data may inform genetic disorders or predisposition to specific illnesses), as well as information about an individual's blood relatives. The key challenge of using genetic data in biomedical research lies in its higher potential for identification of a range of related individuals, especially those who consented to research participation under anonymity and their family members who may not be aware and/or may not have consented to contributing to the research.[15]

9.20 Collection, storage, and dissemination of genetic information are associated with high risks of re-identification since the information garnered is unique, personal, and challenging to adequately anonymise. It could also lead to inadvertent profiling of individuals, where biases are formed against those who are found to be more genetically susceptible to certain medical conditions (e.g., certain ethnic groups that are more susceptible may be the target of bias, see Chapter 6: Responsible Data Usage). As the use of genetic information is often left to the user's discretion, there could be unspecified downstream use of the genetic data that contributors may not have consented to.[16] For instance, broad consent, as an alternative to study-specific consent, permits researchers to engage in research use of participants' de-identified genetic data without the requirement to obtain additional consent for future storage, maintenance, or secondary research uses of the data, so long as the future activities are within the scope of the broad consent.[17] Researchers may leverage data from multiple sources to yield new insights, which then increases the risk of re-identification. Researchers should therefore evaluate the risk of re-identification and appropriate safeguards should be put in place.

[15] Conboy, C. (2020). Consent and Privacy in the Era of Precision Medicine and Biobanking Genomic Data. *American Journal of Law & Medicine, 46*(2–3), 167–187. https://doi.org/10.1177/0098858820933493

[16] Wan, Z., Hazel, J.W., Clayton, E.W. et al. (2022). Sociotechnical safeguards for genomic data privacy. *Nat Rev Genet*, *23*, 429–445. https://doi.org/10.1038/s41576-022-00455-y

[17] Attachment C - Recommendations for Broad Consent Guidance (2017 Edition). Secretary's Advisory Committee on Human Research Protections (SACHRP). https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-c-august-2-2017/index.html

9.21 While genetic data is widely recognised as sensitive data, the crucial question is whether all genetic data is necessarily and always identifiable. Determining the status of genetic data i.e., whether and under what conditions it should be considered as identifiable, has significant implications for researchers who use and share such data. For example, processing identifiable data would require an appropriate legal basis, such as consent given, and adequate organisational and technical safeguards in place. It is moot if consent must also be obtained from potentially identifiable blood relatives. This would quickly be impracticable from a researcher's perspective, and potentially intrusive of relatives' privacy too. On the contrary, irreversibly de-identified (or anonymised) data is not considered personal data and is not subject to the PDPA in Singapore. One key factor that impinges on the identifiability of genetic data is the context of the genetic data.[18] The characteristics of specific genetic datasets, such as the type of data (e.g., germline versus somatic tumour variants, non-coding versus coding deoxyribonucleic acid (DNA)), sample size, or rarity of the genetic variant considered, represent a key factor for assessing the likelihood of re-identification. For example, non-identifiable genetic data may include anonymised or aggregated partial genetic sequences or genetic test results that can no longer be practicably linked back to a specific genetic identity, sample or profile, a patient record, or to any other identifier.

9.22 In deliberating whether genetic data should be considered exceptional and treated differently from other types of personal and health data, the following ethical principles could be considered:

a. The principle of *respect for persons* requires that research institutions and researchers place importance on the welfare and concerns of individuals whose genetic data is used, given that genetic data is sensitive personal data with implications for the individuals and their family members. Researchers should also adequately communicate to participants the research intent, anticipated individual, familial and/or societal impacts, how their genetic data will be used and the risks of re-identification of genetic data, before obtaining their consent for the use of their genetic data in biomedical research. These include contacting blood relatives of participants whose data is being used for the research study and informing them of the way the data will be used, potential relevance or impact to them and other risks of data re-identification.

   Respect for persons is a key principle but is not absolute. Researchers should balance an individual's interests (e.g., protection of privacy of research participants' genetic data) with the wider public interests and societal benefits, and in this context, this includes the research participants' family's interests. Incompatible or irreconcilable ethical perspectives could be resolved with some regard for public interest. It requires the sharing of data for research (e.g., open access) to promote collective benefit.

b. The principle of *proportionality* requires that the anticipated risks (e.g., identification of research participants from their genetic data) and extent of regulation of biomedical research involving genetic data are appropriate, in

[18] Shabani, M. & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation. *EMBO Rep*, *20*(6), e48316. https://doi.org/10.15252/embr.201948316

relation to the research intent and proportionate to the potential benefits to the participants and society. For instance, with increasing use of genetic data, the risk of re-identification of 'anonymised' data also increases which affects research participants, and their family members. To mitigate such risk, researchers could control data access through enhancing the security level of the system and assessing the relevance of the user requesting access.[19]

c. The principle of *justice* requires that researchers offer the benefits from biomedical research to individuals whose genetic data was used in that research, where appropriate and applicable, and that researchers and their institutions incur some responsibility for the welfare of participants in the event of adverse outcomes arising directly from their participation in the research (e.g., a participant's genetic data has led to his/her identification and that of his/her family members and the researcher should inform the participant and affected family members of potential risks of data re-identification and remain responsible in ensuring fair data usage and safeguarding their welfare). As genetic data may also reveal the participants' genetic susceptibility to certain medical conditions, the principle of *justice* requires researchers to strive to manage and use genetic data in a responsible way that does not create or reinforce biases or discriminatory profiling or worsen healthcare equity and result in unfair health outcomes for already disadvantaged groups. One way to lower the risk of data re-identification of participant and/or their families is by excluding identifiable information (e.g., the relationship of each participant's relative) into a database. Researchers who require the data could contact the repository under a confidentiality agreement.

Examples of Large-scale Biomedical Research Initiatives Using Big Data

Global Initiative on Sharing Avian Influenza Data (GISAID)[20]

GISAID was formed during the 61st World Health Assembly in May 2008 as a publicly accessible database for scientists to improve the sharing of data of all influenza viruses (and more recently, the coronavirus causing COVID-19). This includes genomic sequences and related clinical and epidemiological data associated with human viruses, and geographical as well as species-specific data associated with avian and other animal viruses, to aid in disease surveillance and tracking of outbreaks, and to help researchers understand how viruses evolve and spread during epidemics and pandemics. This is achieved by ensuring open access to the database for biomedical research use.

Since early 2020, GISAID has become the world's largest genome sequence database with over ten million genomes as of May 2022. This has enabled scientists to rapidly access sequences from the database to aid in their analysis and understanding of how viral variants evolve or spread during epidemics and pandemics, and promoted influenza research, for example, the development of drugs and/or vaccines using the sequence data.

[19] Takashima, K., Maru, Y., Mori, S. *et al*. (2018). Ethical Concerns on Sharing Genomic Data Including Patients' Family Members. *BMC Med Ethics 19*, 61. https://doi.org/10.1186/s12910-018-0310-5

[20] Global Initiative on Sharing Avian Influenza Data (*GISAID). (2022). Global Initiative on Sharing Avian Influenza Data (GISAID).* Retrieved December 25, 2022. https://gisaid.org

Genomics England 100,000 Genomes Project[21] – UK

The 100,000 Genomes Project, managed by Genomics England, was established in 2013 to sequence 100,000 genomes from ~85,000 National Health Service (NHS) patients affected by rare diseases or cancers. It is focused on rare diseases and cancers as both are strongly linked to changes in the genome. The project aims to make genomics part of routine healthcare by working closely with the NHS to integrate whole genome sequencing (WGS) and enhance genomic healthcare research by creating the largest genomic healthcare data resource in the world to enable discoveries for current research participants and future generations through genomic-level analysis of diseases.

For instance, a pilot study of rare undiagnosed diseases that analysed the genes of 4,660 people from 2,183 families (all of whom were early participants in the 100,000 Genomes Project) using WGS led to a new diagnosis for 25% of the participants. Of these new diagnoses, 14% were found in regions of the genome that would be missed by conventional methods, including other types of non-whole genomic tests. Recruitment for the study was completed in December 2018 and results from the project are currently being returned to participants. Beyond direct results, researchers continue to use data from the project to develop new treatments, diagnostics, devices, and medicines.

[21] Genomics England. (2022). 100,000 Genomes Project. *Genomics England.* Retrieved December 25, 2022. https://www.genomicsengland.co.uk/initiatives/100000-genomes-project

CHAPTER 10: REVISITING CONSENT IN THE ARENA OF BIG DATA AND AI

This chapter discusses the various types of consent in the context of biomedical research and the major challenges that may impede informed consent with respect to big data. Ethical issues/considerations pertaining to consent in the use of big data are also discussed.

10.1 Consent could be classified as implied, broad, specific, explicit, and dynamic. A research participant may express broad (general) consent to allow personal information to be collected, used and stored for biomedical research whereas specific consent could be provided through opt-in or opt-out mechanisms for research studies.[1] Dynamic consent is a more engaging approach where research participants are provided with information on research use(s) of their biospecimens, health and personal data before consent is obtained through communication via a secure digital platform. Such approach allows individuals to revisit and review consent decisions and preferences over time.[2]

10.2 In reference to BAC's 2021 Ethics Guidelines, the BAC recommended specific consent for personal information be sought and applied for a specific project, and for broad consent to be sought in cases where personal information could be used also in future projects. IRBs should hold the discretion to decide if specific consent is required, or if a previously given broad consent is sufficient for the research project. For consent involving vulnerable persons (e.g., persons lacking mental capacity, minors, and persons whose autonomy might be prejudiced by being under the influence of third parties), BAC has called for additional safeguards such as the involvement of the deputy/donee/guardian in decision-making, consent to be taken by independent third parties, and the assurance of safety should research participation be declined. These safeguards apply under the prevailing consideration of research that does not involve more than minimal risk and are for the participants' best interests.[3] A role for consent remains a viable governance tool in the context of big data and AI use in biomedical research because - where it is feasible to obtain - informed consent suggests that a research participant has acquired sufficient understanding (i.e., the participant has been explained of the research project and processes, the benefits and risks of participating in the research, his/her right to withdraw from the study at any time) and has authorised the use of his/her data for biomedical research.

10.3 There are, however, three major challenges that may impede obtaining of informed consent from research participants with respect to big data use, which are discussed as follows:

a. One possible challenge that impedes the obtaining of informed consent from research participants in the context of big data use in biomedical research is

[1] Willison, D.J., Swinton, M., Schwartz, L. *et al.* (2008). Alternatives to Project-Specific Consent for Access to Personal Information for Health Research: Insights from a Public Dialogue. *BMC Med Ethics, 9*, 18. https://doi.org/10.1186/1472-6939-9-18

[2] Teare, H.J.A., Prictor, M., & Kaye, J. (2021). Reflections on Dynamic Consent in Biomedical Research: The Story So Far. *Eur J Hum Genet* 29, 649–656. https://doi.org/10.1038/s41431-020-00771-z

[3] Bioethics Advisory Committee. (2021). Ethics Guidelines for Human Biomedical Research (2021 Revised). *Bioethics Advisory Committee.* Retrieved February 12, 2023. https://www.bioethics-singapore.gov.sg/publications/reports/bac-ethics-guidelines-2021

transparency. The concern of *transparency* arises when internal workings, such as algorithms and software used in AI, are not revealed to, or understood sufficiently by, research participants. A lack of information because of a lack of *transparency* is entirely inimical to a valid consent (or valid refusal). This problem can be obstinate due to the nature of some of the AI technology which does not make its working 'knowable'.

b. Another challenge arises when re-purposing extant data for other research which occurs when AI algorithms are applied to existing datasets for analysis. This may require obtaining re-consent from individuals from whom the information was collected for secondary purposes.

c. Lastly, the lack of provision of other meaningful alternatives to potential research participants may impede the obtaining of informed consent from them. Individuals will be deprived of their prerogative to negotiate if they do not completely agree with the terms of agreement.

Issue 1 – What are the differences between forms of consent taking for health and medical data (defined as data pertaining to or informing of one's health) that are collected via various sources and novel methods?

10.4 Traditionally, personal and medical data providing information on patient health may be obtained from sources such as research studies and healthcare institutions. The collection, access and use of such data is often underpinned by laws and regulatory frameworks where informed consent of research participants is taken explicitly, rather than implicitly or by other models of consent. This requires that the participants be fully informed about the nature of the data that is being collected, the purpose of the data collection, and the potential risks and benefits of participation in the research. Individuals should also be informed that they may withdraw from the research at any time without having to provide any explanation or justification, and without penalty or prejudice to any treatment they may be receiving (also mentioned in BAC's 2021 Ethics Guidelines).[3] Such a consent taking process is based on the ethical principle of *respect for persons*, where an individual is treated with respect and there is an attendant commitment to respect their autonomy, and is given the opportunity to make informed choices regarding participation in biomedical research.

10.5 With advancements in technology, health information may also be derived from novel methods such as consumer platforms, social media, wearables, and sensors. The data of research value, while centred around individuals, is often generated from multiple sources. Consent for mobile data collection is often carried out through the internet of things (IoT) or edge computing, which is also known as 'instant' data or real-time data generated by sensors or users, where data can be processed more quickly and closer to where it is generated, allowing real-time interaction with users. This is unlike cloud computing which processes large datasets on centralised remote servers, making real-time interaction difficult. In such scenarios, obtaining informed consent in the manner where patients and individuals can understand clearly and sufficiently how their data will be used becomes very challenging. In many cases, individuals already provide valid consent for the use of their personal data by accepting click-wrap agreements where the terms are written in technical jargon with insufficient explanation. Individuals may not read or comprehend these agreements before consenting. As such, it is important to provide more information on the use of personal data in the user agreements for clarity. However, it is not assured that reliance on these kinds of click-wrap terms would be ethically robust enough to cover future uses of data for research purposes.

10.6 While an appropriate online informed consent procedure may not easily replace in-person procedures, the ethical principle of *respect for persons* remains a key consideration. Informed consent for use of data derived via novel methods such as consumer information and sensor data may be obtained using technology to tailor consent procedures to the level at which research participants wish to be informed. In cases where the researcher has oversight of the consent taking process, he/she should take extra care to contextualise and assess the amount of information to inform the individual or disclose for correct interpretation based on the individual's preferences prior to data collection. Always, however, there must be sufficient information and understanding to constitute *valid* consent.

10.7 As the use of big data increases in biomedical research, studies have also noted a growing trend of using 'decentralised data' in research. Decentralised data refers to data generated from multiple sources or decentralised platforms such as digital health mobile applications or a combined data repository. Given the sheer volume and pace of data generation, there are challenges, including appropriate data governance, data tracking and data audit process arising from the use of decentralised data. Decentralised data does not have a central authority or entity[4] that is responsible to track and audit the data. The data is also often fragmented and lacks standardisation, which makes it difficult to analyse and interpret and raises questions about data quality. To manage decentralised data, a robust data governance framework is needed. This framework should address issues related to privacy, security, ownership, and consent. It should also provide mechanisms for tracking and auditing the data. Clear policies and protocols for data sharing should also be established. The FAIR Data Principles (Findable, Accessible, Interoperable, and Reusable) are widely accepted as a set of best practice guidelines for the preparation of data for sharing, and the management of data with the protection of privacy and confidentiality of research participants in mind (see Chapter 7: Data Ownership, Custodianship and Stewardship for more information).

10.8 Consent processes for the use of data derived via various sources and novel methods may need to be contextualised appropriately by researchers and/or their institutions so that research participants have sufficient understanding and information before providing consent to participate in ongoing research investigations and provide data that would be useful for biomedical research.

Issue 2 – What are the limits of consent and what is the role of waiver of consent?

10.9 Informed consent from research participants entails procedures to limit deception and coercion.[5] However, informed consent can only be obtained when the individual

[4] Inery. (2022). Centralized VS. Decentralized Database Management. *Inery*. Retrieved March 29, 2023. https://inery.io/blog/article/centralized-vs-decentralized-database-management/

[5] O'Neill, O. (2003). Some Limits of Informed Consent. *Journal of Medical Ethics, 29*(1), 4–7. https://doi.org/10.1136/jme.29.1.4

is competent and capable of giving valid consent. Nonetheless, biomedical research may involve participants who may be cognitively impaired or lack formal legal capacity at the time of consent taking. It is thus important to consider not only the ethical principle of *respect for persons* but additional factors which limit consent taking:

a. **Vulnerable groups (persons who lack mental capacity, minors, highly compromised individuals) who cannot give valid consent:** BAC's 2021 Ethics Guidelines stipulates that for minors and for persons lacking mental capacity, the parents of the minor or deputy, or donee may decide on the individual's participation in the biomedical research. The BAC also recommended that consent be taken by independent third parties for vulnerable populations such as highly compromised patients whenever possible, especially in cases where the attending physician is also the researcher.

10.10 For healthy individuals or research participants, there could be a limitation in their understanding of research and risks and benefits of data use. For instance, some may not fully understand the scope of the research, the risks, or the potential consequences of their data being used, especially in highly complex biomedical research such as AI or genetic research. Researchers should provide clear and understandable information about the research, including its purpose, procedures, risks, and benefits. The information should be presented in ways that are accessible to the participants, using language appropriate for their level of understanding. Furthermore, researchers should offer opportunities for participants to ask questions and seek clarifications about the research and the consent process. This can help to ensure that participants fully understand what they are agreeing to and their involvement in the research. As time is often required to understand the research study, researchers should also allow participants time to review the information before deciding on participation. Participants should not be pressured or rushed into making a decision.[6] It is also crucially important that those seeking consent explain what is not known or knowable with AI, e.g., how the technology works or other aspects of the technological processes. These are 'known unknowns' that are also part of a robust consent process.

10.11 It can also be difficult for research participants to control how their data is used or shared as the research progresses or when data is used for secondary purposes. The option for complete withdrawal of the participant's data may not be possible especially when the data is shared across multiple projects or research groups. In the EU, there is precedence that the withdrawal of consent would not affect the results of activities already carried out, including the storage and use of data obtained based on informed consent before withdrawal.[7] It is recommended that consent is not relied upon as the basis to conduct lawful processing of data for research purposes. Rather, some other legal basis is preferred, such as public interest.

[6] Manti, S., & Licari, A. (2018). How to Obtain Informed Consent for Research. *Breathe*, *14*(2), 145–152. https://doi.org/10.1183/20734735.001918

[7] Official Journal of the European Union - Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on Clinical Trials on Medicinal Products for Human Use (2014). *European Commission*. (2014, May 27). Retrieved February 25, 2023. https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf

10.12 In the biomedical research context in Singapore, there are situations warranting waiver of consent. A waiver of consent requires researchers to seek approval from an ethical review body (typically an IRB) to use an individual's personal data in the proposed research without obtaining his/her consent. In deciding when to apply waiver of consent, the ethical principles of *respect for persons* and *solidarity* need to be considered by the researcher. The principle of *respect for persons* is not violated if waiver of consent would not adversely affect the welfare and interests of research participants and if the research does not pose more than minimal risk to the participants. The IRB, which is the reviewing authority for human biomedical research, should also consider these ethical principles when making an independent assessment on whether to allow waiver of consent for the proposed research.

10.13 The principle of *solidarity* recognises that while individuals have the right to control use of their personal data, there are also situations where it is in the public interest of society as a whole to allow access to data for research that would benefit the public.[8] The duty of easy rescue, a moral principle that suggests that individuals have an obligation to help others who are in distress when the cost of help is relatively low, could also be used to justify the waiver of consent requirements, for example, for minimal risk research/studies.[9]

10.14 In Singapore, the BAC recommends that waiver of consent may be considered if the following conditions are met: (i) The research is justified and poses no more than minimal risk to research participants; (ii) The waiver will not adversely affect the welfare and interests of research participants; (iii) The research could not practicably proceed without the waiver; (iv) Obtaining consent is not possible or practicable; and (v) Individual privacy and confidentiality of the personal information are assured.[3] This is aligned with the Fifth Schedule of the Human Biomedical Research Act (HBRA),[10] which stipulates that IRBs can approve requests to waive informed consent if the following additional conditions are satisfied: (i) the individually-identifiable health information were obtained or compiled before 1 November 2017; and (ii) the research cannot reasonably be carried out without the use of the health information in an individually-identifiable form.

10.15 Other instances where waiver of consent may be warranted in the use of big data and AI for biomedical research include mining data from large pools of data from various sources, for which informed consent would be difficult to obtain.[11] Waiver of consent may also be considered for biomedical research projects that serve the public interest or demonstrate some level of societal value, when consent, anonymisation

[8] IRB-Health Sciences and Behavioral Sciences (IRB-HSBS), University of Michigan (2023). Waivers of Informed Consent Guidelines. *Research Ethics & Compliance, University of Michigan*. (2020, August 19). Retrieved February 12, 2023. https://research-compliance.umich.edu/waivers-informed-consent-guidelines

[9] Porsdam Mann S., Savulescu J., & Sahakian B. J. (2016). Facilitating the Ethical Use of Health Data for the Benefit of Society: Electronic Health Records, Consent, and the Duty of Easy Rescue. *Philosophical transactions. Series A, Mathematical, Physical, and Engineering Sciences, 374*(2083), 20160130. https://doi.org/10.1098/rsta.2016.0130

[10] Human Biomedical Research Act 2015 (2020 Revised Edition), Fifth Schedule, 'Waiver of Requirements for Appropriate Consent by Institutional Review Board'. *Singapore Statues Online*. https://sso.agc.gov.sg/Act/HBRA2015

[11] ReCODE Health. (2017). Understanding "Consent" in the Age of Big Data and Human Research. *ReCODE Health*. (2017, June 12). Retrieved February 12, 2023. https://recode.health/2017/06/12/understanding-consent-age-big-data-human-research/

or participant's benefit cannot be met.[12] One study reported that among 1,988 randomised controlled trials (RCTs) published from 2014 to 2019, 8% of trials (n=165) waived participants' consent.[13] However, the onus is on the researchers to ensure that there is little or no potential harm to the participants from whom the data was obtained.

Issue 3 – In what ways does consent for use of data differ between cohort studies and that of real-world data?

10.16 Cohort studies typically involve longitudinal studies on a group of individuals to study the development of certain health outcomes, such as the incidence of a disease, and can be retrospective (looking back in time and using existing data e.g., medical records or claims database) or prospective (requiring the collection of new data).[14] They can also be conducted as cross-sectional, case-control, or nested case-control studies. In ensuring that the rights, interests, and welfare of research participants are protected, cohort studies often entail obtaining valid consent explicitly from participants for usage of data in research prior to their participation in research. In cases where it is not possible to obtain informed consent in cohort studies, IRBs may still require consent and provide further guidance to researchers for consent taking or approve requests for waiver of consent for research to be carried out in the public interest (see para 10.15).

10.17 However, obtaining consent for the use of real-world data[15] (collected from a variety of sources, such as electronic health records, insurance claims data, and data from health-monitoring devices) can be more challenging, because the data is often not collected primarily for research purposes and there are considerable practical difficulties in suitably informing citizens of what might happen to their data. There is ongoing debate about whether the current practice of consent taking for cohort studies or for health and medical data is applicable for real-world data.[16] The main challenges of obtaining consent for real-world data include:

a. **Secondary use of data**: As real-world data is often collected for a specific purpose (e.g., service evaluation or clinical management), individuals may not be aware that their data could be used for secondary purpose in research. Such secondary use of data has become increasingly common in recent years, as advances in technology and data science have made it possible to extract more value from existing real-world datasets. One approach is to obtain broad consent at the time of data collection, where individuals are asked to consent

[12] Schaefer, G.O., Laurie, G., Menon, S. *et al.* (2020). Clarifying How to Deploy the Public Interest Criterion in Consent Waivers for Health Data and Tissue Research. *BMC Med Ethics* 21, 23. https://doi.org/10.1186/s12910-020-00467-5

[13] Dal-Ré, R. (2023). Waivers of Informed Consent in Research with Competent Participants and the Declaration of Helsinki. *Eur J Clin Pharmacol*, *79*, 575–578. https://doi.org/10.1007/s00228-023-03472-w

[14] In cohort studies, data is collected in an experimental, interventional, controlled or randomised controlled trial (RCT) setting where data is collected based on variables that are controlled or monitored. [Also mentioned in Chapter 4]

[15] Real-world data is data that is not collected under experimental, or interventional, or controlled conditions, i.e., data not collected in the context of a RCT, but data generated in routine care or clinical practice or data generated from the delivery of healthcare in non-controlled settings. [Also mentioned in Chapter 4]

[16] Lipworth, W. (2019). Real-World Data to Generate Evidence About Healthcare Interventions. *Asian Bioethics Review*, *11*(3), 289–298. https://doi.org/10.1007/s41649-019-00095-1

to the use of their data for a range of research purposes.[17] Often, broad consent needs to be accompanied by good governance mechanisms to ensure adequate oversight and ongoing protection of the individual's personal data in its secondary uses. An alternative is to obtain specific consent for each research study that will use the data, which may be operationally challenging due to the large sample size, time required, possible resource constraints (e.g., limited manpower) and/or because the data subjects may not be traceable.

b. **Identifiability of data:** In many cases, real-world data is collected in ways that make it difficult or impossible to completely de-identify the data (e.g., electronic health records). Identifiability is an important consideration because it can affect the level of risk that individuals face when their data is used for research. In big data research, this risk can be amplified because the range of data uses is potentially very wide and hence, the risk of re-identification is raised. While researchers may be able to use statistical methods to reduce the risk of re-identification, such as by removing direct identifiers and aggregating data before analysis, there may still be a risk of re-identification (see Chapter 11: Responsibility to the Public in Data Sharing for Research for more discussion on data de-identification). This calls for the need to ensure *transparency* on the level of identifiability of the data and the potential re-identification risks involved in using the data for research when obtaining consent for real-world data collection.[18] Specific consent may be required particularly if the data is highly identifiable or if the research involves potentially sensitive information (such as genetic and genomic data) or if the risks of future re-identification are particularly high.

c. **Large-scale studies:** Real-world data used in public health and clinical research among other fields, is often collected on a large scale, which can make obtaining individual consent impractical due to the sheer volume of data involved. As real-world data can often come from many different sources, such as electronic health records and personal health and activity monitoring tools, or different sectors and/or countries, identifying each individual and obtaining their consent can be difficult or even impossible. In many cases, especially for retrospective studies, the data may already exist and be stored in various databases, making it difficult to obtain retrospective consent from each individual source and obtaining consent from each individual may also be time-consuming and expensive. This can delay research and ultimately limit the amount of new knowledge to be gained from the data.

10.18 Given these challenges, obtaining consent for using real-world data for research can be complex and different from that of cohort studies. Taking the principle of *proportionality* into consideration, IRBs should decide if specific or broad consent is appropriate for biomedical research involving personal information, regardless of data sourced from cohort studies or real-world data and differences in the extent of de-identification and advise researchers on the suitability of the de-identification measures taken, while weighing the level of care and urgency required based on the

[17] Mikkelsen, R. B., Gjerris, M., Waldemar, G. *et al*. (2019). Broad Consent for Biobanks is Best – Provided it is also Deep. *BMC Medical Ethics, 20*(1). https://doi.org/10.1186/s12910-019-0414-6

[18] El Emam, K., Jonker, E., Arbuckle, L. *et al*. (2011). A Systematic Review of Re-Identification Attacks on Health Data. *PLoS ONE*, *6*(12). https://doi.org/10.1371/journal.pone.0028071

sensitivity of the data. This is in contrast with the US Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,[19] where covered entities may use or disclose health information that is de-identified without restriction (including patient's authorisation) for research as it is not considered protected health information (PHI). Such entities must ensure the health information is sufficiently de-identified by removing the 18 identifiers/elements as enumerated in the Privacy Rule. An exception is provided when waiver of consent is allowed, which is explained in *Issue 2* above. Research which relies exclusively on the secondary use of irreversibly de-identified information may qualify for an exemption from ethics review, as stated in BAC's Ethics Guidelines 2021.[3]

10.19 As such, alternative consent models such as dynamic or broad consent, may be more appropriate for real-world data.[2, 20] These modes of consent, however, would likely result in significant economic and transaction costs. It is important for IRBs to provide oversight and ensure that research using real-world data is conducted in an ethical and responsible manner, with appropriate data governance and privacy protections in place.

[19] Office for Civil Rights. (2017). HIPAA for Professionals: Research. *U.S. Department of Health and Human Services (HHS).* (2017, December 18). Retrieved March 23, 2023. https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

[20] Richter, G., Krawczak, M., Lieb, W. *et al*. (2018). Broad Consent for Health Care–Embedded Biobanking: Understanding and Reasons to Donate in a Large Patient Sample. *Genetics in Medicine*, *20*(1), 76–82. https://doi.org/10.1038/gim.2017.82

CHAPTER 11: RESPONSIBILITY TO THE PUBLIC IN DATA-SHARING FOR RESEARCH

This chapter discusses the need for responsible data sharing, and its importance to individuals, communities, and society. Ethical issues and considerations pertaining to benefit sharing with research participants whose data is used are also discussed.

11.1 Biomedical research has been growing at an increasingly rapid pace over the past few decades, with key developments in the field being driven by technological advancements in artificial intelligence and big data.[1] These advances have been dependent on the availability of large volumes of data from many individuals and diverse sources, achieved through data sharing among researchers and the general public.

11.2 The sharing of biomedical research data is increasingly viewed as a moral duty.[2] Data sharing has the potential to accelerate scientific progress, optimise the value of data, and promote scientific integrity. The combination of even larger datasets into big data offers even greater benefits for science, medicine, and society.[2] Sharing of data increases data circulation and use by encouraging greater transparency, enabling reproducibility, and allowing for greater understanding of the subject matter for both researchers and the public.[3] Data sharing also enhances efficiencies, increases collaboration among research institutions, and allows easier access to research. These in turn, facilitate the public understanding of research data use, enable meaningful results, accurate predictions of health data trends, diagnoses, and facilitate decision-making as well as encourage innovation and advancement in research.

11.3 Increasingly, many research funding agencies require data generated from grant funded projects to be made publicly available to enhance open access to research data. Many agencies have also instituted requirements for data sharing and formal data management plans. For example, the National Medical Research Council (NMRC) in Singapore developed a 'Framework for Research Data Sharing and Governance' to cover broad principles on research data sharing. The Framework requires NMRC-funded projects to allow open access of research outcomes to peer-reviewed publications and share final research data for high value projects (i.e., $250,000 and above). The growing expectation for researchers to share their data also highlights the need for responsible data sharing.

11.4 While responsible data sharing can lead to research that benefits individuals, communities and society as a whole, ensuring quality data sharing for research is conducted ethically, equitably, and with proper respect for privacy presents major

[1] Xu, Y., Liu, X., Cao, X. *et al.* (2021). Artificial Intelligence: A Powerful Paradigm for Scientific Research. *The Innovation, 2*(4), 100179. https://doi.org/10.1016/j.xinn.2021.100179

[2] Kalkman, S., Mostert, M., Udo-Beauvisage, N. *et al*. (2019). Responsible Data Sharing in a Big Data-Driven Translational Research Platform: Lessons Learned. *BMC Medical Informatics and Decision Making, 19,* 283. https://doi.org/10.1186/s12911-019-1001-y

[3] Data Republic (2020). The Importance of Data Sharing for all Organizations. *Data Republic.* (2020, April 7). Retrieved April 15, 2023. https://datarepublic.com/resources-guides/the-importance-of-data-sharing-for-all-organizations

challenges.[4] It is essential to consider key ethical principles such as *justice* and *solidarity* in data sharing for research to help address these challenges. For instance, the principle of *justice* would be an important consideration in ensuring the fair treatment of research participants and that resources or benefits yielded from the research are allocated equitably. Researchers have the duty to share data and to ensure that only high-quality data is shared for scientifically valid proposals. Systems for data sharing should allow for efficient use, and be highly interoperable and accessible, as well as sustainable for the future. Effective mechanisms for benefit sharing will need to be in place to ensure fair distribution of risks, benefits, and burdens. On the other hand, the principle of *solidarity* requires researchers to balance societal benefits with the protection of privacy and rights of individual participants when sharing research data, and this will be discussed further in the later part of this chapter.

Issue 1 – How can the benefits of biomedical research be shared widely and equitably, including with participants whose data is used?

11.5 Big data and data analytics have been adopted across the life sciences.[5] Big data in clinical study refers to the information collected using electronic database, and these data come from daily routine clinical practice without modification or screening with strict inclusion and exclusion criteria, therefore retaining its real-world features.[6] Increasingly, researchers are using big data analytics and re-using existing patient data obtained from past clinical trials,[7] and using big data presents possibilities ranging from better patient recruitment and engagement to more efficient trials and better-quality results.[5] This is because big data is routinely collected and often provides better quality information than controlled clinical trials,[5] and big data techniques can allow researchers to analyse data from much larger patient groups than those included in clinical trials, which might reduce bias in results.[8] Biomedical research utilising big data contributed by research participants and patients can generate outcomes that are beneficial to the individual as well as the community.

11.6 Individual-level benefits include improved understanding of results from a clinical trial and pooling of results from multiple trials may generate even deeper insights.[9] Data collected from an individual clinical trial may be re-analysed to derive new information and interpreted to confirm the reproducibility of results which provides research participants and the wider community with more comprehensive knowledge of the trial outcomes that may be used in outlining risks and benefits, including in

[4] Yoong, S. L., Turon, H., Grady, A. *et al.* (2022). The Benefits of Data Sharing and Ensuring Open Sources of Systematic Review Data. *Journal of Public Health, 44(*4), 582-587. https://doi.org/10.1093/pubmed/fdac031

[5] Anju Team (2022). Big Data, Big Benefits: How Third Party Data Can Improve Clinical Trials. *Anju Software*. (2022, October 10). Retrieved April 16, 2023. https://anjusoftware.com/big-data-clinical-trials/

[6] Zhang, Z. (2014). Big Data and Clinical Research: Perspective from a Clinician. *Journal of Thoracic Disease, 6*(12), 1659-1664. https://doi.org/10.3978/j.issn.2072-1439.2014.12.12

[7] MIT Technology Review Insights (2021). Clinical Trials are Better, Faster, Cheaper with Big Data. *MIT Technology Review*. (2021, June 10). Retrieved April 16, 2023. https://technologyreview.com/2021/06/10/1025897/clinical-trials-are-better-faster-cheaper-with-big-data/

[8] Goarnisson, O. (2020). Future Developments in Clinical Studies: Big Data Analysis. *Sidley Austin LLP*. (2020, March). Retrieved April 16, 2023. https://sidley.com/en/insights/publications/2020/03/future-developments-in-clinical-studies-big-data-analysis

[9] Institute of Medicine (US). (2013). Sharing Clinical Research Data: Workshop Summary. *The National Academies Press*. https://doi.org/10.17226/18267

personalised treatments. Individual-level data from several clinical trials may also be merged to derive information via meta-analyses that may differ across sub-groups and to highlight patterns not realised previously. Meta-analyses done with individually identifiable patient data are more likely to observe treatment effects that differ across subgroups[9] and allow diagnostic accuracy to be estimated at the level of relevant patient subgroups,[10] than meta-analyses done with aggregate data. This would be useful in informing research participants of the research outcomes and enable them to make informed decisions pertaining to their clinical treatment or management. However, the latter analysis would require the data being analysed in circumstances when it is not fully anonymised. Here it is a matter of balance and trade-offs between risks and benefits.

11.7 Even when analysed in aggregated form to protect privacy, data contributed by individual research participants can prove useful to derive wider trends in the community. Sharing of aggregated data can bring about wider communal benefits, such as informing risk/benefit analysis of treatment options and identifying trends from previous studies. Making information available to the public also deters selective and inaccurate reporting of research outcomes by ensuring that research outcomes are reproducible and helps to accelerate research. In situations where it may be difficult to interpret conflicting data from clinical trials, data sharing enables proper data analysis by confirming reproducibility of results or highlighting to researchers whether conflicting results are due to chance or true differences.[9] This in turn, generates information and research outcomes that inform decision-making and benefit the wider community.

11.8 Although data sharing could bring about individual-level and communal benefits, it also poses risks to individuals contributing their data. This is because there is challenge in preserving privacy while maximising the access of big data for research, given that privacy concerns are more prominent in large, diverse datasets, which increasingly track nuanced detail of participant behaviour, and pose increased risk of revealing personally identifiable sensitive information, as compared to small datasets that can be more easily de-identified.[11] In addition, obtaining specific consent when using big data in biomedical research might be difficult due to the high number of data subjects involved, and in cases where research is conducted on large-scale repositories, it might not be completely feasible to recontact all data subjects and inform them that the purpose of data processing has changed from the original consent agreement stipulated at the time when the repository was created.[12] Therefore, sharing of big data brings new ethical responsibilities to safeguard individual's privacy, and it would be important to find solutions to preserve privacy, while still allowing biomedical science the fundamental ability to learn, access, and replicate findings.[11]

[10] Broeze, K. A., Opmeer, B. C., Van der Veen, F. *et al.* (2010). Individual Patient Data Meta-analysis: A Promising Approach for Evidence Synthesis in Reproductive Medicine. *Human Reproduction Update, 16*(6), 561-567. https://doi.org/10.1093/humupd/dmq043

[11] Crosas, M., Gary, K., James, H. *et al.* (2015) Automating Open Science for Big Data. *The ANNALS of the American Academy of Political and Social Science, 659*(1), 260-273. https://doi.org/10.1177/0002716215570847

[12] Ferretti, A., Ienca, M., Hurst, S. *et al.* (2020). Big Data, Biomedical Research, and Ethics Review: New Challenges for IRBs. *Ethics and Human Research, 42*(5), 17-28. https://doi.org/10.1002/eahr.500065

11.9 Researchers and institutions should, to the best of their abilities, consider the ethical principle of *solidarity* when sharing research data. *Solidarity* is defined as a shared commitment within a community – such as research participants - to accept some potential individual costs to yield the accepted benefits for the greater good of the public. In the context of biomedical research, it considers the importance and need to balance societal benefits and ensuring the welfare and well-being of the general public with the protection of privacy and rights of individual participants. As *solidarity* also considers the public value that specific instances of data use create (i.e. data use creates public value when it benefits people and communities without posing grave risks), it acts as a catalyst to data justice by facilitating good data use, protecting individuals from harm, and ensuring that benefits are shared with the public.[13] Researchers have the responsibility to ensure that their research outcomes benefit the wider society, and that their research outcomes and research data are communicated and shared with the general public.[14] If a research finding is found to have important implications to the public, researchers have an obligation to relate this new knowledge to society such that the general public can make informed decisions.

11.10 Given the availability of large amounts of biological and clinical data that have been generated and collected at an unprecedented speed and scale,[15] and the ability for the use of big data in biomedical research to produce better quality results,[5] the need for researchers to fulfil their social responsibility would prompt them to conduct more biomedical research using big data. Such big data applications present new opportunities to discover new knowledge and create novel methods to improve the quality of clinical care, and while sharing of research outcomes and data could benefit the public, it would come at the expense of research participants' privacy, given the difficulty in obtaining specific consent for big data use in biomedical research. However, researchers have a responsibility towards research participants, which includes protecting the rights and welfare of participants and ensuring the integrity of participants' data.[16] Therefore, it would be important for researchers to balance their responsibility to the public and their research participants, by applying the ethical principle of *solidarity*.

11.11 Further to adhering to the principle of *solidarity*, research institutions and researchers should have processes or mechanisms in place to ensure responsible sharing of data and reduce the risk of individual re-identification. These include assessing and regularly reviewing the risk of re-identification through (i) identifying data elements in a research dataset that overlap with external data sources, (ii) identifying small classes of records defined by unique combinations of those data elements, and (iii) considering the likelihood of population overlap between research dataset and an

[13] Prainsack, B., El-Sayed, S., Forgo, N. *et al*. (2022). Data Solidarity: A Blueprint for Governing Health Futures. *The Lancet Digital Health, 4(*11), 773-774. https://doi.org/10.1016/S2589-7500(22)00189-3

[14] Society for Neuroscience. (1999). Responsible Conduct Regarding Scientific Communication. *The Journal of Neuroscience, 19*(1). https://doi.org/10.1523/JNEUROSCI.19-01-j0003.1999

[15] Luo, J., Wu, M., Gopukumar, D. *et al*. (2016). Big Data Application in Biomedical Research and Health Care: A Literature Review. *Biomedical Informatics Insights, 8*, 1-10. https://doi.org/10.4137/BII.S31559

[16] David, B. R. & Ness, E. (2012). Participants' Responsibilities in Clinical Research. *J Med Ethics, 38*(12), 746-750. https://doi.org/10.1136/medethics-2011-100319

external source, followed by applying the appropriate risk mitigation strategies,[17] explaining the risk to participants when obtaining informed consent prior to collection of personal data for biomedical research purposes, and controlling access to data that could potentially identify individuals. In situations where it would be not possible or practicable to obtain consent from research participants regarding the use of their data in biomedical research, IRBs may waive consent requirements for the use and sharing of data obtained from participants, provided the data is irreversibly de-identified and there is no possibility of re-identifying the individuals who had contributed the data.

11.12 IRBs and research institutions should also ensure that adequate provisions to protect the privacy of research participants and the confidentiality of data are in place and that there are also processes for monitoring the data collected, such as accurate recording of all adverse events and reviewing other applicable datasets to ensure participants' continued safety. Given that re-identification is becoming gradually easier because of big data due to the abundance and constant collection and analysis of information along with the evolution of technologies and the advances of algorithms,[18] it would be important for researchers and research institutions involved in data generation to take the necessary precautions to reduce the risk of individual re-identification and ensure responsible sharing of research data.

11.13 In addition, research funding agencies can work to protect the interests and anonymity of individuals while enabling biomedical research that benefits the wider society. This can be done through developing frameworks such as codes of practice for research data sharing to better guide institutions and investigators on handling of research data, as well as impose sanctions that are proportionate to the nature of the offence, such as a withdrawal of funding, if researchers deliberately attempt to re-identify individuals from anonymised data or negligently expose them to the risks of re-identification.

11.14 It is also of key importance to promote Open Science among researchers, which encompass a range of practices aimed at making science more reliable, including wider sharing and reanalysis of code, data, and research materials, valuing replications and reanalyses, interactive and more transparent ways of presenting data graphically and open access publishing.[19] Open science practices increase efficiency and quality of research, allows for an expansion of innovation, and promotes collaboration. With increased access to publications and journals, duplication of research, as well as the cost of creating and reusing data can be reduced.

11.15 In short, the potential benefits of data sharing extend to individual and communal levels. Given the fundamental shift in the nature of big data and the pressing challenges in the field of big data use in biomedical research such as data privacy

[17] Simon, G. E., Shortreed, S. M., Coley, R. Y. *et al*. (2019). Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care Records. *The Journal of Electronic Health Data and Methods, 7*(1):6. https://doi.org/10.5334/egems.270

[18] CaseGuard (2021). Using Re-Identification to Manage Risk, Data Privacy. *CaseGuard*. (2021, January 12). Retrieved April 16, 2023. https://caseguard.com/articles/re-identification-manage-your-risks/

[19] Christopher, A. & David M. A. M. (2019). Open Science Challenges, Benefits and Tips in Early Career and Beyond. *PLoS Biology. 17*(12). https://doi.org/10.1371/journal.pbio.3000246

and integrity,[20] it would be important to govern data sharing activities in a responsible way by balancing societal benefits, ensuring fair distribution of risks, benefits and burdens, respect for individuals and groups including the need to respect for privacy and confidentiality as well as continued stakeholder engagement. Appropriate governance framework and mechanisms should be established so that data sharing can ensure the well-being of the general public while protecting the privacy and rights of individual participants. In addition, researchers and institutions should adhere to other key ethical considerations. These considerations include accountability, transparency, integrity, and professionalism in ensuring responsible data sharing in research and addressing challenges from varying levels and requirements of de-identification. The roles and responsibilities of IRBs should be clearly determined and may include monitoring compliance with policies and regulations for 'data sharing' in research and managing datasets that are not governed by any system for data sharing. These in all, would help in the development of a harmonised governance framework for big data sharing in biomedical research.

[20] Cremin, C. J., Dash, S., & Huang, X. (2022). Big Data: Historic Advances and Emerging Trends in Biomedical Research. *Current Research in Biotechnology, 4,* 138-151. https://doi.org/10.1016/j.crbiot.2022.02.004

CHAPTER 12: USE AND STORAGE OF LEGACY AND POSTHUMOUS DATA

This chapter discusses the importance of the use of legacy and posthumous data, the issues relating to the proper storage and use of such datasets in human biomedical research, the relevant Acts and guidelines put in place to ensure the proper and ethical use of these datasets, the ethical implications involved in their use, including posthumous medical data donation (PMDD) activities and the return of posthumous data to family members, and the need for researchers and institutions to consider various ethical principles when using legacy and posthumous datasets.

Introduction

12.1 Progress in biomedical sciences has been furthered through the availability, sharing and use of personal data from patients and healthy individuals participating in biomedical research. With the availability of accumulated and archived datasets acquired over years, researchers are also provided with the option of using such datasets for research purposes, which further increases the efficiency and effectiveness of biomedical research. However, consent models for some of these datasets may have become obsolete.[1] In addition, the biomedical research landscape is changing. More longitudinal studies and long-term biomedical research projects are being conducted, and the follow-up period required for research participants in such studies can range from as short as a few weeks to as long as several decades. This presents the likelihood of a research participant passing away during a long-term study, especially for research involving participants with high mortality risks such as advanced cancer or cardiac disease.[2] However, most research policies and consent forms currently do not address the use of data after a participant's death and/or the use of data long after consent was obtained and might have expired. These issues have led to growing concerns regarding legacy[1] and posthumous data use[2], which warrant the need for researchers and institutions to consider effective mechanisms to ensure the ethical storage and management of legacy and posthumous datasets.

Legacy Data

12.2 Legacy data refers to (i) data in datasets previously obtained or used for research, and/or (ii) datasets generated from legacy or archival biological samples, and/or (iii) clinical data obtained and retained from experiments without specific or adequate consent for research. Some of these datasets may have been irreversibly de-identified, which makes it impossible or impractical to trace the donors (if living) for consent. In situations where legacy datasets are large-scale and complex, these datasets can be described as 'Big Data' and are potentially useful in analysis, as such data can also be recoded, integrated, and aggregated, as well as reinterpreted

[1] Wallace, S. E., Kirby, E., Knoppers, B. M. *et al.* (2020). How Can We Not Waste Legacy Genomic Research Data? *Frontiers in Genetics*, *11*. https://doi.org/10.3389/fgene.2020.00446

[2] Bak, M. A. R., Ploem, M. C., Blom, M. T. *et al.* (2020). Stakeholders' Perspectives on the Post-mortem Use of Genetic and Health-Related Data for Research: A Systemic Review. *European Journal of Human Genetics 28*(4), 403-416. https://doi.org/10.1038/s41431-019-0503-5

according to changing scientific paradigms.[3] As obtaining new data prospectively may require a large amount of time and effort and/or might be impracticable, for certain projects biomedical research could be accelerated by using legacy data from previous research studies. In some cases, legacy data may have been created before widespread data sharing was encouraged or made available. In these earlier times, research proposals and consent materials did not include provisions to enable further sharing, and often included conditions that limited the way in which a researcher could use or share datasets.[1] Hence, contemplating biomedical data (including genomic data) being shared for secondary research purposes could be more intricate for existing legacy data, as researchers may not know whether these data meet current ethical and regulatory requirements for sharing. In situations where further use of legacy data is ethically justified, the use of biomedical data beyond their original purpose should not impact the efficiency and productivity of further biomedical research. However, if legacy data is not allowed for use even in ethically justified situations, researchers may need to spend more time and resources conducting new and unnecessary research studies for new data collection, instead of analysing and using existing legacy data.[4]

Posthumous Data

12.3 Posthumous data refers to personal data, which includes but is not limited to medical, clinical research, financial, social media, government, and tax data relating to deceased persons. Posthumous data can also be classified under legacy data. However, posthumous data relates specifically to the deceased, unlike legacy data which can relate to both the living and the deceased. Posthumous data pertaining to one’s health and medical conditions may be donated and used for purposes of medical research. This is known as posthumous medical data donation (PMDD).[5] Benefits of PMDD include supporting advanced and personalised medical research, and providing a basis for data mining, machine learning and AI, generating new understanding of chronic diseases, such as cancer and mental illness.[6] Posthumous data might also be used when the wishes of the deceased are not known, subject to appropriate safeguards. However, given that posthumous data can be highly sensitive, it would be important for researchers to treat such data with exceptional care where the context so requires.[7]

[3] Schofield, P. N., Kulka, U., Tapio, S. *et al.* (2019). Big Data in Radiation Biology and Epidemiology; An Overview of the Historical and Contemporary Landscape of Data and Biomaterial Archives. *International Journal of Radiation Biology*, *95*(7), 861-878. https://doi.org/10.1080/09553002.2019.1589026

[4] Pronk, T. E. (2019). The Time Efficiency Gain in Sharing and Reuse of Research Data. *Data Science Journal*, *18*(1), 1-8. https://doi.org/10.5334/dsj-2019-010

[5] Pearce, H. (2022). Our Data? An examination of the Possible Role of Individual Consent in the Regulation of Posthumous Medical Data Donation (PMDD). *Computer Law & Security Review, 45.* https://doi.org/10.1016/j.clsr.2022.105663

[6] Harbinja, E. & Pearce, H. (2020). Your Data Will Never Die, But You Will: A Comparative Analysis of US and UK Post-Mortem Data Donation Frameworks. *Computer Law and Security Review, 36.* https://doi.org/10.1016/j.clsr.2020.105403

[7] Bak, M. A. R., & Willems, D. L. (2022). Contextual Exceptionalism After Death: An Information Ethics Approach to Post-Mortem Privacy in Health Data Research. *Science and Engineering Ethics, 28.* https://doi.org/10.1007/s11948-022-00387-0

Legislation Governing the Use and Storage of Legacy and Posthumous Data

12.4 To ensure the proper collection, use and handling of legacy data, specifically posthumous data, by researchers and institutions, relevant legislation has been put in place in Singapore. For example, Section 31(e) of the Medical Registration Act 1997 (MRA) requires that the Registrar of the Singapore Medical Council remove the name of any medical practitioner who is deceased, along with his/her addresses, qualifications and other particulars from the register of medical practitioners.[8] In addition, the Human Biomedical Research Act 2015 (HBRA) sets out provisions regarding posthumous data use, including that consent for the use of a deceased person's individually-identifiable health information or removal or use of tissue from the deceased person for research purposes must be obtained from appropriate persons (i.e., a spouse, adult son or daughter, parent or guardian, an adult brother or sister, administrator or executor of the estate of the deceased person, or individuals authorised to dispose the body of the deceased) under Section 11 of the Act.[9] Lastly, Section 51 of the Healthcare Services Act 2020 (HCSA) requires that medical information in medical records or information relating to the condition, treatment or diagnosis of deceased persons should not be disclosed unless consent from the representative of the deceased, such as his or her executor, administrator or next-of-kin, is obtained.[10] While there are legislative provisions specifically for the use and storage of posthumous data, there is currently no Singapore legislation governing the use and storage of other legacy data obtained from donors who are still alive.

Ethical Frameworks and Guidelines for Legacy and Posthumous Data Use and Storage

12.5 In some jurisdictions, regulatory guidelines and frameworks have been put in place to ensure the ethical use of legacy data, particularly posthumous data. For example, the Code of Ethics on Posthumous Medical Data Donation was developed by the Digital Ethics Lab at the Oxford Internet Institute to state the fundamental ethical principles which should govern all PMDD activities. This was in recognition that PMDD activity constitutes an act that is both meaningful to an individual and valuable to the public. The guiding ethical principles are: (i) human dignity and respect for persons; (ii) promotion of the common good; (iii) respecting citizens' right to participate and collaborate in scientific research; (iv) quality and good data governance; and (v) transparency, accountability, and integrity.[11] The BAC has also provided recommendations on the applicable ethical principles for IRBs to consider when reviewing and approving data management arrangements in its 'Personal Information in Biomedical Research (2007)' report. In the case of deceased persons whose information may be retained in a database, access for research should be a matter for the custodian of the information, having regard to any explicit objection by the persons prior to their death. The custodian should also ensure that procedures

[8] Medical Registration Act 1997 (2020 Revised Edition), Section 31: 'Alterations in Registers'. *Singapore Statutes Online*. https://sso.agc.gov.sg/Act/MRA1997

[9] Human Biomedical Research Act 2015 (2020 Revised Edition), Section 11: 'Consent for Research or Removal or Use of Tissue for Research in Case of Deceased Persons'. *Singapore Statutes Online*. https://sso.agc.gov.sg/Act/HBRA2015

[10] Healthcare Services Act 2020, Section 51: 'Confidentiality of Information, etc'. *Singapore Statutes Online.* https://sso.agc.gov.sg/HSA2020

[11] Krutzinna, J., Taddeo, M., Floridi, L. *et al.* (2019). An Ethical Code for Posthumous Medical Data Donation. *The Ethics of Medical Data Donation, 12*, 181-195. https://doi.org/10.1007/978-3-030-04363-6_12

for obtaining consent related to deceased participant data are stated upfront.[12] BAC's guidelines complement Singapore's legislations i.e., MRA 1997 and HBRA 2005 by further setting out recommendations on database custodianship that guides institutions (data custodians), on their responsibilities in the storage and management of legacy and posthumous data.

12.6 There are currently limited frameworks and guidelines on the storage and ethical use of other legacy data in biomedical research that are stored in databases such as those obtained from donors who are still alive. However, given that it would be impossible to remove or erase legacy data from databases as data might have been replicated across multiple research studies, and that the value of such datasets might have diminished or nullify over time, these factors would need to be considered when putting in place any robust ethical approaches or recommendations to managing and using legacy and posthumous data for biomedical research. Traditional approaches, such as a role for consent or re-consent, might have little or no role and therefore, a first principles approach is required to reflect on what is important in determining whether and how such data can and should be used.

Ethical Principles for Legacy and Posthumous Data Use and Storage

12.7 Further to the relevant legislation, ethical frameworks and guidelines that govern the use and storage of legacy data, specifically posthumous data, researchers and institutions should consider the following ethical principles when using and storing legacy and posthumous datasets:

a. The principle of *respect for persons* requires that the welfare and concerns of individuals whose personal data are used in biomedical research are protected as far as possible, even after death. In the context of PMDD, as retrieving specific consent for unforeseen secondary uses of data obtained through PMDD activities would not be possible, such data could be misused to justify unfair public policies or profiled beyond biomedical research purposes.[13] As such, using posthumous data in these circumstances would violate the dignity of the donor and should be discouraged. In addition, given that retrieval or use of data of deceased persons might emotionally burden their family members, it is also important to respect family members' decisions when they do not want posthumous data of their deceased kin to be retrieved or used,[2] particularly when no previous decision was registered, or no explicit consent was given by the deceased donor.[14] Furthermore, using legacy data for which no specific or adequate consent was previously obtained or if consent models have lapsed or become obsolete, this would also infringe the living donors' rights and compromise the interests of the deceased. While obtaining consent or re-consent for the use of such data may not be possible given that most

[12] Bioethics Advisory Committee. (2007). Personal Information in Biomedical Research. *Bioethics Advisory Committee*. Retrieved April 8, 2023. https://www.bioethics-Singapore.gov.sg/publications/reports/personal-information-in-biomedical-research

[13] Krutzinna, J., Taddeo, M., & Floridi, L. (2019). Enabling Posthumous Medical Data Donation: A plea for the Ethical Utilisation of Personal Health Data. *The Ethics of Medical Data Donation, 11*, 163-180. https://doi.org/10.1007/978-3-030-04363-6_11

[14] Rosenblum, A. M., Horvat, L. D., Siminoff, L. A. *et al.* (2012). The Authority of Next-of-Kin in Explicit and Presumed Consent Systems for Deceased Organ Donation: An Analysis of 54 Nations. *Nephrol Dial Transplant, 27*(6), 2533-2546. https://doi.org/10.1093/ndt/gfr619

legacy data cannot be retrospectively re-consented,[3] this does not mean that such data can never be used. For instance, in cases where a future use was never contemplated or refused, the ethical justification must be particularly strong, such as in promoting common good and benefits to the general public to warrant the use of such datasets.

b. The principle of *proportionality* entails that the risks in biomedical research should be proportionate to the potential benefits to the participants or others. While it may be important to protect posthumous interests – application or fulfilment of interests occurs after a person's death,[15] the use of legacy and posthumous data for research may be considered when the potential benefits generated outweigh the risk of infringing such posthumous interests. For example, there may be circumstances when the disclosure or the use of legacy and posthumous data in biomedical research is required to save the immediate life or prevent the occurrence of diseases by facilitating the development of cures and treatments. These appeals to the common good may potentially outweigh the need to respect the former interest of the deceased in protecting the confidentiality of his personal health information and preserving his own identity and reputation.[15] In such instances, the use of these datasets would be justifiable. In addition, the effect of time elapsing from the moment of death on the extent of disclosure and use of legacy and posthumous data should also be considered. The period of protection required for these datasets needs to take into account the need to protect privacy interests of surviving relatives, and the need for archivists and others to access old records on deceased individuals for historical purposes. These considerations would also justify the use of the datasets for research purposes after the protection period has ended.

c. The principle of *sustainability* supports arguments for the fair and just conservation of nature and minimisation of resource depletion for the good of the planet. In consideration of mankind's responsibility for future generations, researchers should as far as possible, reduce the environmental impact of big data and AI systems to ensure that research processes and outcomes do not unfairly jeopardise or prejudice the welfare of future generations. With more legacy and posthumous data being retained for biomedical research purposes, some of these datasets may not be accessed for years, or long periods of time. Therefore, it would be important to ensure that they are stored in an efficient and sustainable manner that reduces carbon footprint and energy consumption[16] to enable effective storage and management of these datasets over longer life cycles, so that in future, when the need arises, they can be used to facilitate research in the development of medical treatment for diseases and benefit future generations.

Mechanisms for Proper Handling, Use, and Storage of Legacy and Posthumous Data

12.8 Given that the issue of data confidentiality applies even after death, IRBs as the gatekeepers to ensure data confidentiality, should be responsible in protecting the

[15] Sperling, D. (2006). Posthumous Interests: Legal and Philosophical Examination in the Medical Context. *TSpace Repository*. (2006). Retrieved April 14, 2023. https://hdl.handle.net/1807/119866

[16] Pure Storage (2022). Reducing the Environmental Impact of Data Storage. *Unsustainable Magazine*. (2022, June 11). Retrieved April 17, 2023. https://unsustainablemagazine.com/environmental-impact-of-data-storage/

values and preferences of the deceased. IRBs could require that researchers adequately inform or ask research participants for their consent and preference for posthumous disclosure of findings to relatives or the use of posthumous data in biomedical research during the initial consent taking process.[2]

12.9 IRBs could also be the authority to make decisions pertaining to the access and use of legacy and posthumous data, especially when no decision was previously made by the deceased participant,[2] taking into consideration the ethical principles of *respect for persons* and *proportionality*. For example, consent requirements for the use of legacy data for biomedical research may be waived if it is irreversibly de-identified and there is no possibility of re-identifying the individuals who have contributed the data. For research studies using identifiable legacy data obtained from donors who are still alive, but where it is impossible or impracticable to seek their consent, IRBs should ensure that adequate safeguard measures are in place to protect donors' privacy and the confidentiality of any personal information associated with the data.

12.10 Principal investigator of a research study also has the responsibility to justify that the public interests or benefits in the study's results outweigh the living donor's right for privacy and the need to protect posthumous interests, and that there is no alternative way to answer the study question for their study, in order for the study to be ethically approved by an IRB.[17] In addition, a special advisory board may also be set up as the overall decision-making authority over any access requests to PMDD databases to ensure that access to PMDD is only granted for scientifically and ethically approved research.[11]

12.11 Other effective mechanisms that could be put in place to enable researchers and institutions to conduct research using legacy and posthumous data ethically include processes for identifying, reporting, managing, and investigating incidents such as breaches, losses of data, or unauthorised access. Proper record-keeping and access management should also be maintained to ensure the integrity of the PMDD and protection against unauthorised access to any PMDD. Additionally, researchers and institutions should de-identify PMDDs using prevailing standards, avoid any re-identification of data, and use adequate and updated encryption techniques to ensure safe and secure storage of PMDD to minimise the risk of unauthorised access, data loss, or misuse.[11]

12.12 In addition, researchers and institutions should store legacy data properly to ensure that such data is well-preserved and available for use in the future, as legacy data without proper documentation and storage (e.g., data recorded on obsolete digital storage media) is at greater risk of being lost and would in any event also become effectively useless. This could be done by archiving legacy data, which is the process of storing no longer actively used data such that it becomes easily discoverable and reliably retrievable in the future.[18]

[17] Shaw, D. M., Gross, J. V., & Erren, T. C. (2016). Data Donation After Death: A Proposal to Prevent the Waste of Medical Research Data. *EMBO Rep*, *17*(1), 14-17. https://doi.org/10.15252/embr.201541802

[18] Renaut, S., Budden, A. E., Gravel, D. *et al.* (2018). Data Management, Archiving, and Sharing for Biologists and the Role of Research Institutions in the Technology-Oriented Age. *BioScience. 68*(6), 400-411. https://doi.org/10.1093/biosci/biy038

12.13 In summary, the proper handling and use of legacy and posthumous data could facilitate significant advances in biomedical research. However, the issues arising from the use of such data would have to be considered by IRBs, researchers, and institutions when handling and using these datasets. IRBs, researchers, and institutions should consider the ethical principles of *respect for persons*, *proportionality*, and *sustainability* in addition to complying with the relevant legislation and ethical guidelines to ensure the legal and ethical use and storage of legacy and posthumous datasets. In the near future, general data donation schemes may enable people to donate all their personal data after death, similar to existing practices of organ or body donation. Indeed, such data donation schemes have already been established for certain datasets, such as full genomes donated through the Personal Genome Project. As more dataset types follow suit, it will be critical for researchers and institutions to establish appropriate mechanisms to govern PMDD activities, to ensure the ethical use of PMDD in biomedical research.

CHAPTER 13: ETHICAL CONSIDERATIONS AND ISSUES SPECIFIC TO AI

This chapter discusses ethical issues and considerations specific to AI, with the goal of enabling researchers, institutions, stakeholders, and users to develop an understanding of AI technologies' capabilities, their potential impact to society, and challenges and ethical issues.

13.1 With advancements in technology, the use of AI in biomedical research is becoming increasingly prevalent. Digital technologies such as sensors and wearables may be employed to gather health data from patients and individuals accurately and in real time, enabling researchers to harness valuable information from big data. The information obtained may be used to generate observable patterns and trends in diseases to inform individual and population level research. While leveraging on AI may potentially accelerate biomedical research and advance progress in medicine through better understanding of human health, there are also challenges and ethical issues to be addressed.

13.2 The lack of clarity or consensus on the meaning of principal ethical issues and values, such as privacy, bias and explainability, when applied to AI in biomedical research, is a major concern. The Nuffield Foundation has identified three key issues: (i) No agreement around key ethical concepts and their application; (ii) lack of attention on conflicts between ideals and values; and (iii) lack of evidence of AI's capabilities and the way it is perceived by the public.[1] The Nuffield Foundation recommends that there should be a common understanding of frequently employed key AI concepts and terms by various stakeholders of society (e.g., machine learning researchers, social scientists, lawyers, ethicists, philosophers, etc.). Multidisciplinary and multi-sectorial engagements, through regular meetings and conferences, will help to resolve ambiguity and facilitate communication among these parties. Tensions that may arise, due to conflicts in values and principles within Singapore's biomedical research community, regulators, developers, technology providers, clinicians, and patients, should be identified and addressed through having a deeper understanding of the technological capabilities of the algorithms in place, their impact on the society and considering perspectives from the aforementioned stakeholders. Ensuring openness and transparency in communications and AI processes is also required at all stages of AI development and/or use and stakeholders should adhere to key ethical principles and values in ensuring transparency in the development processes.

13.3 Ethical principles that may apply to AI in biomedical research include but are not limited to transparency, explainability, and justifiability. Other key considerations include reliability and safety, accountability, proportionality, human agency, equitable access, and model security to minimise potential harm to individuals and parties involved in research projects.[2]

[1] Whittlestone, J. Nyrup, R. Alexandrova, A. *et al*. (2019). Ethical and Societal Implications of Algorithms, Data, and Artificial Intelligence: A Road Map for Research. *London: Nuffield Foundation.* Retrieved March 20, 2023. https://www.nuffieldfoundation.org/sites/default/files/files/Ethical-and-Societal-Implications-of-Data-and-AI-report-Nuffield-Foundat.pdf

[2] Feizmann, H., Villaronga, E. F., Lutz, C. *et al*. (2019). Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns. *Big Data & Society, 6*(1). https://doi.org/10.1177/2053951719860542

Issue 1 – Transparency, explainability and justifiability of AI

13.4 Researchers should consider the ethical principles of *transparency*, *explainability* and *justifiability* in the development and use of AI in biomedical research which are important in reducing biases in AI algorithms and making the system more transparent, explainable and auditable.[3] *Transparency* refers to the need to openly inform and communicate with various stakeholders, at all stages of the AI system's development and implementation, how the AI system is designed, developed and applied. *Explainability* of AI systems refers to the interpretability of input, output, and behaviour of the AI model and how it contributes to the outcome of the prediction. An *explainable* AI model enables biomedical researchers, users, and patients to understand the AI models' predictions and how the outcomes were derived. While not all AI models are inherently *explainable* or can be explained by modern algorithms, researchers should consider the application of *explainable* methods when conceptualising new AI models. The ways in which *transparency and explainability* will apply and impact various stakeholders are discussed as follows:

a. **Government regulators**: Researchers should be transparent with regulators on how data will be procured and processed. They should also be transparent on why a specific AI algorithm is chosen, how the AI model is going to be developed and the extent of the AI model's validation. They should disclose the results of their surveillance and monitoring of the AI model's performance as it is applied. *Transparency* ensures prompt action by regulators to intervene and address issues where necessary, at all stages of AI model development and implementation. Nonetheless, even when researchers are transparent with disclosing the AI algorithms and models that they used for research, regulators will not be able to regulate what they cannot understand and interpret. By being able to interpret the models independently from what the researchers have reported, regulators will be able to make an assessment on the safety and reliability of the models for biomedical research.

b. **Scientific communities**: The objective of the peer review process is to assess the originality, validity, significance, and reproducibility of research. This process cannot be completed without adequate transparency and access. Therefore, researchers should endeavour to release anonymised and de-identified datasets and use open-source AI algorithms and models, for the purposes of allowing other researchers within their scientific communities to reproduce, verify and build on their findings. In addition, by ensuring e*xplainability* of the AI system, the scientific community will be able to interpret the AI algorithms and models in the context of known scientific knowledge, for the purposes of determining the originality and contribution of the reported research. This is critical as not all AI algorithms and models will perform better than traditional statistical learning methods e.g., logistic regression models.

[3] Organisation for Economic Cooperation and Development (OECD). (2019). OECD AI Principles: Transparency and Explainability (Principle 1.3). *OECD.AI Policy Observatory*. Retrieved March 18, 2023. https://oecd.ai/en/dashboards/ai-principles/P7

c. **Developers and clinicians**: *Transparency* on the performance of the AI algorithms and models is important for developers and clinicians to demonstrate trustworthiness in the safety and reliability of the technology. Without the crucial element of trust, developers will not be able to develop their research projects into complete products and clinicians will not be willing to apply the research outcomes and the developers' products on their patients. When developers and clinicians apply AI algorithms and models, it is paramount that they contextualise the technology in relation to the product or clinical application they intend to develop and use. To do this, there must be sufficient understanding of why the AI agent makes a specific prediction or recommendation. A good understanding can help developers and clinicians nuance their decisions and be cautious of edge cases in which there can be failures in the AI technology or where the technology generates outcomes that still involve uncertainty and require more human judgment.

d. **Patients**: Being open and transparent to patients that they are interacting with AI or that their treatments are based on an AI technology will also help to promote patient's trust and enhance AI's credibility as a critical tool that can help them improve their health. It also enables patients to provide feedback to regulators, researchers, developers, and clinicians should there be evidence that the AI algorithms and models are not preforming as expected. Patients should also be informed of why a particular prediction, diagnosis or treatment was recommended by an AI agent to enable them to influence more control of their own health.

13.5 Justifiability refers to the assessment of whether the decisions of an AI system are valid or reasonable based on the rules and norms of society.[4] Justifiability is often erroneously deemed to be synonymous with explainability. While explainable AI is focused on facts, justifiable AI is focused on judgment. It is important that the outcomes of AI decision making can be independently justified using plausible ethical principles and values. This is so that the well-being and autonomy of subjects involved in the research studies are taken into consideration, and *accountability* is attributed to parties contributing their personal data.[5] It will also be easier to identify limitations and safer for people working with the system to handle and use the system when they can understand the justifications of the AI's decisions.

Challenges of 'Black Box AI' Systems

13.6 In the use of AI, a phenomenon known as the 'Black Box AI' may arise when methods for explaining, monitoring, and troubleshooting AI models and algorithms are hard to develop in parallel to AI models and algorithm research. 'Black Box AI' refers to AI models that give an incomplete view to users or another interested party

[4] Hadfield G. K. (2021). Explanation and Justification: AI Decision-Making, Law, and the Rights of Citizens. *Schwartz Reismen Institute of Technology and Society*. (2021, May 18). Retrieved March 19, 2023. https://srinstitute.utoronto.ca/news/hadfield-justifiable-ai

[5] Muralidharan A., Schaefer G. O., Savulescu J. (2022). Three Observations about Justifying AI. *British Medical Journal*. (2022, March 2). Retrieved March 19, 2023. https://blogs.bmj.com/medical-ethics/2022/03/02/three-observations-about-justifying-ai/

of the processes and workings between inputs and outputs[6]. Some examples include ensemble decision trees (algorithms which combine multiple decision trees to produce higher predictive performance), support vector machines (algorithms that search for the optimal hyperplane for linearly separable patterns) and deep learning with artificial neural networks (algorithm that contain multiple hidden layers of nodes that process the given inputs to produce an output prediction). As AI is not error-free and it cannot be easily probed since not all AI is interpretable, humans often cannot understand how AI derives its conclusion, but can only view the conclusion/output.[7] Therefore, biased AI systems which are not detected by researchers, users and patients might perpetuate biases, leading to discriminatory decisions. This is particularly risky in healthcare where a flawed AI-based decision (i.e., medical diagnosis via AI) may have a significant impact on someone's health or life or increase risks of discrimination during insurance applications or employment.

13.7 To reduce or avoid undesirable implications brought about by 'Black Box AI', researchers should conduct research and continue development efforts in explainable AI solutions. Explainable AI is an area of AI that seeks to develop processes and methods allowing a human to understand the results and output created by machine learning algorithms. One of the many ways it does so is by estimating individual attributes' expected impact on AI predictions. An example is estimating the impact of an individual's blood pressure (individual attribute) on the AI prediction of the individual's likelihood of having a heart attack. Through explainable AI's characterisation of the model's predictions, researchers can make an assessment on the fairness and the reasonableness of the AI model's predictions and whether it meets regulatory and societal standards.[8] Essentially, the logic of an AI system should be expressed in a comprehensible, human-readable format, that highlights biases learned by the model, so as to allow AI developers and other stakeholders to understand and validate its rationale for making meaningful and fair decisions. Explainable AI can be crucial in earning trust and confidence as it helps users to avoid using AI models (prior to introduction of use) if they are causing harm (*non-maleficence*) and places the responsibility of using AI models and algorithms on the AI user (*accountability*).

13.8 Nevertheless, explainable AI is not perfect and there are limitations of its use. Often, there exists a trade-off between predictive performance and model interpretability of outcomes generated through AI decisions. For instance, while one decision tree is easily interpretable, highly predictive ensemble methods consisting of hundreds or even thousands of decision trees cannot be easily explained. Another example is artificial neural networks, where they are inexplainable by default and modern post-hoc explainable AI methods that might be applied on them are computationally expensive.[9] Given these limitations, unexplainable AI should be applied with caution

[6] Yaser K. (2023). Black Box AI. *TechTarget*. (2023, March). Retrieved March 19, 2023. https://www.techtarget.com/whatis/definition/black-box-AI

[7] Miller K. (2021). Should AI Models Be Explainable? That Depends. *Machine Learning.* (2021, Mar 16). Retrieved March 20, 2023. https://hai.stanford.edu/news/should-ai-models-be-explainable-depends

[8] IBM. (2022). Explainable AI (XAI). *IBM Watson*. Retrieved March 20, 2023. https://www.ibm.com/sg-en/watson/explainable-ai

[9] Izumo, T., & Weng, Y. H. (2022). Coarse Ethics: How to Ethically Assess Explainable Artificial Intelligence. *AI and Ethics, 2,* 449–461. https://doi.org/10.1007/s43681-021-00091-y

since unconscious or algorithmic biases could have been built into AI applications. It is also important that the performance of any AI, interpretable or black box, be evaluated scientifically in ecological environments (i.e., the context or environment which the AI model is built for), ideally through randomised controlled trials to ensure superiority to existing decision-making, no matter how promising computational experiments are of their predictive performance.[10]

13.9 *Explainable* methods can also help to uncover biases within black box AI models. Currently, black box AI models' development is driven by predictive performance and may not be adequate in accounting for other aspects such as fairness and equality, which are particularly important in ensuring stakeholder interests are met. Machines may treat populations with the same characteristics discriminatively, and therefore some AI models may run the risk of replicating and augmenting human biases, especially in minority groups.[11] This could lead to decisions that may have undesirable impacts on certain groups of people if left unchecked. Therefore, it is imperative that operators of AI models identify and address factors that may cause bias through *explainable* methods, for example in word associations and facial recognition technology. In the event that individuals are rendered unjust treatment by the algorithms, early intervention should be carried out by institutions and more research would have to be done to rectify the unfair AI model. Additionally, institutions should implement policies to use *explainable* methods to actively identify discriminative AI models, limit their use and reduce their impact on minority groups.

13.10 In summary, transparency, explainability and justifiability of AI models are important attributes in enhancing fairness, trust and justice in the systems and making them more effective and useful, benefiting various stakeholders such as regulators, researchers, developers, clinicians, and patients. While there are challenges due to the nature of 'Black Box AI', *explainable* AI solutions exist, albeit with limitations. A principles-based approach, as discussed earlier in this chapter should be adopted to ensure that AI is developed and applied ethically.

Example: **UK – National Health Service (NHS) AI Laboratory[12]**

The NHS AI laboratory is a £250 million (SGD $409.95M) investment, that uses AI for early cancer detection, new dementia treatments and more personalised care. It aims to upskill the NHS workforce through the application of transparency and explainability principles so that the workers can use AI systems to provide safe, effective and individualised care for patients.

If the workings of the AI can be easily understood, more workers can be trained to effectively utilise and work alongside AI systems efficiently. This would also empower

[10] Lam, T. Y. T., Cheung, M. F. K., Munro. *et al*. (2022). Randomized Controlled Trials of Artificial Intelligence in Clinical Practice: Systematic Review. *Journal of Medical Internet research, 24*(8), e37188. https://doi.org/10.2196/37188

[11] Lee, N. T., Resnick, P., & Barton, G. (2019). Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms. *Brookings Institution*. (2019, May 22). Retrieved March 20, 2023. https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[12] National Health Service (NHS) England. (2023). NHS AI Laboratory. *NHS England - Transformation Directorate*. Retrieved March 20, 2023. https://www.nhsx.nhs.uk/ai-lab/

workers to be able to troubleshoot or override the decisions of AI systems should an operational conflict arise between human and machine.

Issue 2 – Responsibility to comply with best standards to ensure clinical safety of AI models

13.11 Biomedical researchers and their AI developer partners need to be aware of their ethical responsibilities and adhere to best practices and standards given that research results affect the lives of individuals and the society.[13] They should also ensure that components in research procedures employing AI such as appropriate missing data imputation, model selection, model validation, assurance on model generalisability, comply with local and international guidelines and regulations. Examples of such guidance include MOH's Artificial Intelligence in Healthcare Guidelines (AIHGIe) guidelines and Health Sciences Authority's (HSA) AI-Medical Devices (MD) regulations. This is to promote safe delivery of clinical care with AI models and algorithms.

13.12 There are ethical implications when appropriate standards are not complied with and they are discussed as follows:

a. **Missing data**: Imputation of missing data done by techniques such as 'Multiple Imputation with Chained Equations' generates artificial data points from existing ones to fill in missing data. These artificial data points might lead to bias in the AI model and algorithm and result in wrong clinical predictions and possibly, the causing of harm to patients. However, these issues could be avoided by ensuring that the proportion of missing data to be imputed does not exceed the recommended proportions and that appropriate parameters are used, for the data imputation methodology, as determined by the research community. Failure to proceed in such a way infringes the principle of non-maleficence, where even if there is no benefit to research participants or patients, there should also be no harm done to them.

b. **Model selection**: There is a wide variety of AI models and algorithms that researchers can select from. Furthermore, each of these models and algorithms is associated with a distinct set of hyperparameters (akin to knobs on a machine that can be tuned to adjust the performance of the machine). If models, algorithms and hyperparameters are not tuned appropriately, the impact and benefit of these models would be limited as their performances are not optimised. Failure to comply with model selection standards as stipulated in Singapore's AI Healthcare Guidelines (AIHGle), for example, goes against the principle of beneficence where researchers and clinicians should do their best to maximise benefits for the research participants and patients.

c. **Model validation and generalisability**: Model validation in datasets previously not seen by the AI model is essential to ensure that the AI model can be reasonably generalised for the intended use case and population. It

[13] Gundersen, O. E., & Kjensmo, S. (2018). State of the Art: Reproducibility in Artificial Intelligence. *Proceedings of the AAAI Conference on Artificial Intelligence*, *32*(1). https://doi.org/10.1609/aaai.v32i1.11503

should not work well only under specific conditions predetermined by the researcher. This ensures that: (i) AI models, algorithms and the associated biomedical research are reproducible for further development and innovation by other stakeholders within the ecosystem; and (ii) AI models can be safely applied across multiple and different types of demographics and locations. Failure to perform model validation and ensure model generalisability therefore defies the principles of justice and equity, when biased models can only work for specific populations under certain scenarios. It might also violate the principles of accountability and non-maleficence, particularly when AI models are not validated to be safe for research and clinical application.

Issue 3 – Human agency and oversight in AI

13.13 'Human agency and oversight in AI' refers to AI systems developed and used as a tool that serves people, respects human dignity and personal autonomy, and functions in a way that can be appropriately controlled and overseen by humans. Therefore, it is important that AI systems empower human beings alongside proper oversight mechanisms, achieved through human-in-the-loop, human-out-of-the-loop, and human-in-command approaches. The responsibility of decisions in clinical settings is often accompanied by ambivalence, especially when outcomes generated by AI are taken into consideration during decision making. Hence, the concept of 'diffusion of responsibility' describes scenarios in decision making by AI when different actors and parties are involved, and attribution of responsibility is uncertain and not easily consolidated across multiple parties.[14]AI has yet to achieve the ability to process human emotions and ethics as humans would. Therefore, to avoid any ambiguity in responsibility attribution, the responsibility for AI's wrong decisions should be attributed to:

a. AI algorithm researchers, if the root cause of the wrong decision was found within the original AI research algorithm used to build the model e.g., erroneous code that was widely disseminated;

b. Biomedical researchers, if the source of the error was found to be caused by erroneous adaptation of the original AI research algorithms e.g., inappropriate AI model construction with said algorithms;

c. Developers, if the AI model used to develop the final AI application was erroneously deployed; and

d. Clinicians, if the AI model was used without adequate evaluation of clinical evidence and was applied for the wrong clinical indication.

13.14 People operating and working alongside AI should maintain agency and confidence in AI systems, and institute safeguarding measures based on the ethical principle of *proportionality*. The most optimal model would be to have a human led AI agent with appropriate human oversight mechanisms as discussed earlier. Such an AI agent needs to be adaptable and flexible, allowing users to gain control and override the

[14] Bleher, H., & Braun, M. (2022). Diffused Responsibility: Attributions of Responsibility in the Use of AI-Driven Clinical Decision Support Systems. *AI and Ethics*, *2*(4), 747–761. https://doi.org/10.1007/s43681-022-00135-x

AI system whenever the need arises. It should be created with flexible modes of operation to allow for and incorporate user input as necessary. For instance, if the AI agent performing a surgical operation was found to engage in risky behaviours that might endanger human lives, the system should be adjustable to allow surgeons to override it and assume control of the procedure immediately. If it is a minor deviation, the surgeon's input should be incorporated by the system in real time and the deviation is to be corrected.

13.15 Researchers should consider the values and goals of their stakeholders in relation to the AI system which they are developing. This is because multiple stakeholders and various parties are involved in the procedural nature of AI research, design, development, testing and implementation, such as developers, operators, researchers, research subjects and patients. While AI is widely accepted to make accurate and right decisions given the constraints of the data, such algorithms are often unable to consider factors which are important to the stakeholders. This includes the AI agent's ability to be relatable or understand human empathy and respond to intangible human factors, such as ethical and moral considerations, within the context of many real-life decisions.[15] An example would include the need to adopt a sympathetic approach in deciding clinical treatments for patients by doctors. Hence, researchers should aspire to incorporate ethical values into the design of AI algorithms such that *respect for persons* is maintained. For instance, emphasis could be placed on the specific input parameters of the AI model such as quality of life and patient's personal health goals to ensure that the AI agent does not just optimise survivability over patient's personal comfort and quality of life. Furthermore, institutions may consider putting in place assessment frameworks of AI performance such as AI audit for (i) ethical justifiability of outcomes; (ii) identification of goals or values; and (iii) checking of value alignment with individuals/society, to establish *accountability* to various stakeholders.

13.16 In a clinical trial which is conceptualised to compare the value of AI versus human clinician for clinical decision making, there are concerns relating to the need for safeguards on the AI trial arm to prevent harm to patients. Trial registration is widely considered to improve both transparency and quality of trial reporting and may be put in place to reduce incidence of bias in outcome reporting.[16] At the same time, staff members recruited to handle AI models should be technically trained to evaluate and understand the limitations of these systems for correct and appropriate use. The onus lies on the multiple parties involved in the use of AI in research, such as developers, researchers, healthcare providers and policymakers, to address issues that may arise from its wrongful use.[17]

13.17 In a clinical trial where AI is shown to vastly outperform human clinicians in clinical decision making, the interests of the patients may be prioritised instead. For instance,

[15] McKendrick J., & Thurai A. (2022). AI Isn't Ready to Make Unsupervised Decisions. *Harvard Business Review*. (2022, September 15). Retrieved March 20, 2023. https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions

[16] Won, J., Kim, S., Bae, I. *et al.* (2019). Trial Registration as a Safeguard Against Outcome Reporting Bias and Spin? A Case Study of Randomized Controlled Trials of Acupuncture. *PloS One*, *14*(10), e0223305. https://doi.org/10.1371/journal.pone.0223305

[17] Harvey, H. B., & Gowda, V. (2020). How the FDA Regulates AI. *Academic Radiology*, *27*(1), 58–61. https://doi.org/10.1016/j.acra.2019.09.017

when a novel intervention is shown to vastly outperform the control arm in a clinical drug or medical device trial, the trial is stopped immediately, and the intervention is applied to the entire cohort to benefit as many patients as possible. However, clinical decisions made by AI that may significantly outperform that made by humans during trials should still be supervised by physicians as AI systems are typically built to identify information from trends relevant to the job and would mostly be suited for routine tasks.[18] In such instances, the physician should have no 'treatment preference' throughout the clinical trial if there is genuine uncertainty within the expert medical community about the preferred treatment.[19]

Issue 4 – Equitable access to AI technologies in research

13.18 Developed countries with more advanced technologies that can spearhead developments in AI have increased access to the latest technologies and benefits brought about by AI[20]. Conversely, less technologically developed countries may fall behind in terms of developing helpful AI technologies and in AI advancement and could become dependent on the developed countries for access to such AI technologies. The ethical principle of *justice* suggests the need to enable universal access to latest healthcare technologies such as AI, regardless of nationality, geographical or cultural barriers.[21] Ensuring equitable access to healthcare should also reflect actual needs of care by individuals or various groups of the population. The theory of intersectionality acknowledges the complexity and multidimensionality of people's lives, and posits that the social oppression they may experience might originate from an intersection of different social inequalities and oppressive identities (e.g., race, gender), rather than from a singular marginalised identity.[22] Therefore, while researchers, institutions attempt to make AI agents more accessible to everyone, there are limitations to carrying this out particularly in the consideration of factors such as gender, class, disability, and ethnicity.

13.19 To further address the issue of *equitability*, those responsible for the development of Al models and algorithms would have to consider the following issues:

a. ***Equitability* of research resources:** As there are limited research resources available, research funders often have to prioritise projects based on returns on investment funding, practicability of research outcomes and other factors. The less profitable or less practical research project that might provide sub-maximal benefit to most stakeholders might therefore not be funded impeding research for marginalised groups around the world. Nonetheless, research

[18] Cremer D. D., & Kasparov, G. (2021). AI Should Augment Human Intelligence, Not Replace It. *Harvard Business Review*. (2021, March 18). Retrieved March 20, 2023. https://hbr.org/2021/03/ai-should-augment-human-intelligence-not-replace-it

[19] Freedman, B. (1987). Equipoise and the Ethics of Clinical Research. *The New England Journal of Medicine*. *317*(3), 141–145. https://doi.org/10.1056/NEJM198707163170304

[20] Yu, P. K. (2020). The Algorithmic Divide and Equality in the Age of Artificial Intelligence. *Florida Law Review*. 72, 331–389. Texas A&M University School of Law Legal Studies Research Paper No. 19-44, https://scholarship.law.tamu.edu/facscholar/1439

[21] Daniels, N. (2008). Justice and Access to Health Care. *Stanford Encyclopaedia of Philosophy*. (2008, September 29). Retrieved March 20, 2023. https://plato.stanford.edu/entries/justice-healthcareaccess/

[22] Rai, S. S., Peters, R. M. H., Syurina, E. V. *et al*. (2020). Intersectionality and Health-Related Stigma: Insights from Experiences of People Living with Stigmatized Health Conditions in Indonesia. *International Journal for Equity in Health*, *19*(1), 206. https://doi.org/10.1186/s12939-020-01318-w

funders still have a responsibility to institute responsible and fair funding policies and consider issues of justice and intersectionality in deciding what to prioritise among a research programme and when making individual funding decisions.

b. ***Equitability* in the design and development of the AI models and algorithms:** To design and develop AI algorithms, there must be enough experts ranging from computer science, maths, biology, and medicine who are trained to write or contribute to algorithms that can build the appropriate AI models for biomedical research. In creating AI models, there must also be sufficient resources in terms of computer resource, architecture, hardware, and infrastructure to support the training of large AI models. The disparities between countries in terms of both human capital and resources can lead to a dearth of high quality biomedical and clinical AI products for underdeveloped countries. While many modern AI models and algorithms are open sourced by OpenAI, Meta, Google and other giant technology companies, biomedical AI algorithms and models remain a niche field compared to Large Language Models (LLMs) e.g., ChatGPT, GPT-3 and GPT-4.

13.20 There must be a commitment by countries and companies globally to promote equitable use and access to biomedical AI agents and products regardless of nationality, gender, age, race, language, etc, where AI technology, should be shared as widely as possible. AI technologies should be available for use not only in contexts and for needs in developed countries but also for less developed countries. AI technologies should not encode biases to the disadvantage of identifiable groups, especially groups that are already marginalised. As far as possible, AI technologies should minimise inevitable disparities in power that arise between providers and patients, between policymakers and people and between companies and governments that create and deploy AI technologies and those that use or rely on them. AI tools and systems should be monitored and evaluated to identify disproportionate effects on specific groups of people and not sustain or worsen existing forms of bias and discrimination.[23]This can be achieved through international collaborations, such as through international advisory bodies like International Bioethics Committee (IBC) or the Intergovernmental Bioethics Committee (IGBC) but instituted primarily for the progress of AI. International guidance frameworks to encourage the sharing of beneficial advancements in AI among countries and to address issues of equitable access across countries may also be set out so that further developments in AI for the use in biomedical research is both *responsible* (in terms of what gets funded and safely developed) and *sustainable* (in terms of who gets access to the immediate benefits and also downstream new developments).

Issue 5 – Concept of 'AI model security'

13.21 'AI model security' refers to processes to prevent attacks on AI models and AI model functionality and to protect the confidentiality of sensitive data used to build the

[23] Ethics and Governance of Artificial Intelligence for Health: WHO Guidance (2021 edition), Executive Summary: Ensuring Inclusiveness and Equity. *World Health Organization*. https://apps.who.int/iris/rest/bitstreams/1352854/retrieve

model. It includes proprietary claims in the model itself. Al model attacks may appear in the form of evasion of the model by changing input, altering and controlling of the AI system by corrupting of data and stealing protected information from AI.[24] To ensure 'AI model security', institutions can take steps by first following good cybersecurity and AI governance practices as set out under the MOH's Healthcare Cybersecurity Essentials and Personal Data Protection Commission's (PDPC) AI governance framework, and put in place critical infrastructure with high level of protection available. Traditional application of security safeguard measures such as constant monitoring, analytics and alerts throughout the model development lifecycle improves protection of the model and the data it stores and analyses. Such practices undertaken by research organisations not only promote *accountability* to research participants and regulators but also encourage *transparency* during the development and operating of AI models.

13.22 In today's world, while AI promises to inaugurate a new era of human progress and productivity, provides solutions to complex problems and enhances decision-making and brings about efficiency in research and healthcare developments, there can still be redundancy and worst-case scenarios with AI, particularly the potential for superhuman AI or 'superintelligence', and other brittleness and biases of current machine learning approaches and dangers of over-hyped AI being misapplied. To circumvent these issues, there should be adequate risk assessments and mitigation measures in place where AI systems should be checked for its on-going viability or utility which would be critical in creating or developing a 'rational AI agent' that understands how to take the appropriate actions. Ethics, governance and ownership of the technology (i.e., regulation and oversight of AI, and AI intellectual property) would be key tools to guard against extreme and adverse outcomes from AI and safeguard public interest. These would include developing guidelines and accident investigation processes, protecting individual privacy and public security, designing systems with transparent decision-making, and managing public perception through effective science communication.[25]

[24] Geddes G., & Konrad C. (2020). An Introduction to AI Model Security. *World Wide Technology.* (2020, March 10). Retrieved March 20, 2023. https://www.wwt.com/article/introduction-to-ai-model-security

[25] World Economic Forum's Geostrategy Platform. (2018). How to Manage AI's Risks and Rewards. *World Economic Forum.* (2018, January 11). Retrieved April 17, 2023. https://www.weforum.org/agenda/2018/01/how-to-manage-ais-risks-and-benefits