



IBPRC

International Bioethics and Pandemic Response Cabinet

Agenda:

Addressing Biosecurity Risks and Ethical Challenges in AI-Driven Biological Research and Disease Detection, with Special Emphasis on Algorithmic Bias, Misdiagnosis, and International Governance



DALY COLLEGE MODEL UNITED NATIONS 2026

International Bioethics And Pandemic Response Cabinet

Table of Contents

1.	Letter from the Executive Board
2.	Introduction to the Committee <ul style="list-style-type: none">• About the International Bioethics and Pandemic Response Cabinet• Mandate
3	Background <ul style="list-style-type: none">• Evolution of Biosecurity• Gain-of-Function Research in the Age of AI
4.	Key Issues and Concerns <ul style="list-style-type: none">• Biosecurity and Dual-Use AI in Biological Research• Algorithmic Bias, Misdiagnosis, and Accountability• Ethical Limits of AI• Transparency and Psychological Impact of AI in Healthcare• International Oversight, Transparency, and Regulatory Cooperation
5.	International Frameworks and Regulations <ul style="list-style-type: none">• Existing Bioethics Guidelines• Global Health Governance and Policies• Shortcomings in Regulatory Frameworks
6.	Stakeholder Analysis <ul style="list-style-type: none">• Governments• Healthcare Institutions• AI Developers and Tech Companies• Civil Society and Media

7.	Challenges and Limitations <ul style="list-style-type: none">• Technological Constraints• Ethical Dilemmas• Legal and Regulatory Barriers
8.	Case Studies and Real-World Examples <ul style="list-style-type: none">• United Kingdom• Netherlands and Belgium• Israel• China• Russia• South Korea
9.	Questions a Resolution Must Answer
10.	Conclusion
11.	Guide to Research and Sources
12.	Bibliography



LETTER FROM THE EXECUTIVE BOARD

Dear Delegates,

The Executive Board of the International Bioethics and Pandemic Response Cabinet welcomes you to DCMUN 2026. We are pleased to serve as your Executive Board and look forward to an engaging and productive committee.

Over the course of this MUN, you will deliberate on the agenda:

“Addressing Biosecurity Risks and Ethical Challenges in AI-Driven Biological Research and Disease Detection, with Special Emphasis on Algorithmic Bias, Misdiagnosis, and International Governance.”

This agenda lies at the crossroads of science, ethics, and global governance. The increasing integration of artificial intelligence into healthcare has significantly transformed how diseases are detected, diagnosed, and managed. While these advancements offer opportunities for improved efficiency and innovation, they also introduce important ethical concerns.

AI-driven systems are not inherently neutral. Issues such as algorithmic bias, limited or unequal datasets, and a lack of transparency can result in misdiagnosis and unequal healthcare outcomes. In the context of global health crises, these challenges become even more critical, as decisions made at scale can have far-reaching consequences.

At the same time, the agenda highlights the growing importance of biosecurity. Technologies used in biological research and disease detection can serve both beneficial and harmful purposes. This dual-use nature makes it essential to establish appropriate safeguards while ensuring that innovation is not unnecessarily restricted.

The committee will also explore the human dimension of these developments. The use of AI in healthcare has implications for trust, autonomy, and the doctor–patient relationship. Additionally, its intersection with sensitive issues such as euthanasia raises important ethical questions regarding dignity, consent, and the role of technology in decision-making.

As delegates, you are encouraged to approach this agenda with careful research and thoughtful consideration. A clear understanding of both the technical aspects and the ethical implications will be essential in developing meaningful and practical solutions. This guide is intended to support your preparation, but it should be used as a starting point rather than the sole source of information.

We encourage respectful dialogue, open-minded discussion, and collaborative problem-solving throughout the committee.



As the Executive Board of the International Bioethics and Pandemic Response Cabinet, we will do our best to ensure that this committee is an engaging and enjoyable experience for all of you.

If you have any questions or require our assistance at any point, you can reach out to us at dcmunibprc@gmail.com.

We look forward to working with all of you and making this conference a memorable one!

Chairperson

Aadhya Nahar

Vice Chairperson

Abhyuday Singh

Vice Chairperson

Samaira Jhawar

Rapporteur

Aarav Barjatya



2.Introduction to the Committee

2.1 About the International Bioethics and Pandemic Response Cabinet

The International Bioethics and Pandemic Response Cabinet (IBPRC) lies at the intersection of science, ethics, and global governance. Its main purpose is to address the ethical effects of advancements in healthcare, particularly in the context of global crises such as pandemics.

This committee focuses on two domains: AI-driven healthcare and biosecurity. The influence of artificial intelligence medicine has grown rapidly in recent years, where it is predominantly transforming how diseases are detected, diagnosed, and managed, making it a vital part of future healthcare systems.

AI-driven systems can process vast amounts of data, identify patterns, and generate predictive insights with exceptional speed. In the context of pandemics, within the scope of pandemics, these abilities can greatly improve early detection of outbreaks, optimize resource distribution, and facilitate more effective response approaches.

However, these technological advancements are accompanied by significant ethical challenges. AI systems are not inherently neutral; they are influenced by the data on which they are trained. If this data reflects existing social, economic, or demographic inequalities, AI systems may prolong and amplify these disparities. Reliance on incomplete or biased datasets can lead to serious consequences, including misdiagnosis, delayed treatment, and erosion of trust in healthcare institutions.

This raises critical concerns regarding fairness and the potential for discrimination in healthcare. Alongside these challenges, biosecurity risks have become increasingly prominent. The same technologies that enable rapid medical innovation can also be misused. AI-driven biological research, for example, has the potential to accelerate vaccine development and disease modeling, but it may also be exploited to create harmful biological agents. This dual-use nature of technology makes strong regulatory frameworks and ethical oversight essential to prevent misuse while preserving innovation.

The committee also emphasizes the human aspect of healthcare. Medical decision-making is not purely technical; it involves emotional, psychological, and ethical considerations. The integration of AI into healthcare systems has the potential to reshape the doctor–patient relationship, influence decision-making, and affect individuals' perceptions of their own health, autonomy, and trust in medical institutions.

Furthermore, IBPRC recognizes the global nature of these challenges. Pandemics and technological risks transcend national borders, making international cooperation crucial. Delegates must consider how ethical frameworks and policies can be applied across diverse political, economic, and cultural contexts while ensuring inclusivity and equity.

Finally, the committee adopts a multilateral approach, drawing from medicine, law, philosophy, sociology, and technology. This enables a more comprehensive understanding of bioethical challenges and supports the development of effective and globally relevant solutions.

2.2 Mandate

The IBPRC is a specialised policy simulation cabinet that was established specifically for the purpose of DCMUN 2026. The committee acts as an advisory panel of the international community, comprising members from various countries, public health agencies, bioethics experts, and ethicists. Although the committee lacks any legislative power, it is responsible for developing recommendations and policies related to bioethical and pandemic issues. Our main goal is to create and uphold international bioethical standards that protect human rights, fairness, and accountability during public health emergencies.

The Cabinet establishes guidelines for bioethics on how to allocate vaccinations, financial resources, and data equally, while ensuring that everyone has access to healthcare, especially those who are particularly at risk. It ensures ethical standards are followed, provides policy advice, and oversees pandemic-related research. It also encourages openness, collaboration with other countries, and evidence-based decision-making. It also improves the world's ability to respond to pandemics by providing training, technical support, and building bioethics infrastructure. This makes the response more resilient and based on ethics.

It was established to provide strategic guidance on bioethical principles and frameworks for pandemic preparedness, response, and recovery. We aim to ensure the equitable distribution of medical resources, vaccines, and therapeutic interventions among all member states. The Cabinet also addresses emerging bioethical challenges that arise during infectious disease outbreaks and public health emergencies. In addition, it promotes international cooperation, transparency, and evidence-based decision-making in the governance and management of pandemics.

Its obligations are -

- Member states are required to contribute financial and/or in-kind resources in accordance with their capacities to support the Cabinet's work.
- They are expected to implement their recommendations within their national legislative frameworks and to report on activities related to bioethics compliance and pandemic response.

Furthermore, member states are encouraged to actively support capacity-building efforts and participate in training initiatives to strengthen global preparedness and response systems.

artificial intelligence
ethics
learning
machine
data
healthcare
policy
care
radiology
record
support
deep
social
effectiveness
agents
opportunities
ethical
challenges
impact
values
mental
bioethics
clinical
big
code
risk
electronic
legal
nuclear
regulations
safety
eu
making
principle
system
moral
protection
practice
providers
guidelines
laws
decision
privacy



3. Background

3.1 Evolution of Biosecurity and Bioterrorism

3.1.1 Early Incidents of Bioterrorism and Biological Misuse

Biosecurity started to take shape because of people misusing agents on purpose or by accident. In 1984, some members of a group called the Rajneeshees in Oregon made people sick on purpose by putting Salmonella in salad bars. Over 750 people got sick. It was the first time something like this had happened in the United States. This incident showed that public health wasn't ready for something like this. In 2001, some people sent anthrax spores to the U.S. Senators and media organizations. This resulted in 22 people getting infected and five people dying.

The investigation that followed, called "Amerithrax," found out that the spores came from a research institution that was funded by the government. This showed that people working inside these institutions could be a threat to biosecurity. These events made the United States create the National Science Advisory Board for Biosecurity in 2005.

3.1.2 Emergence of Governance Frameworks

The Asilomar Conference in 1975 was the international meeting to talk about the risks of genetic research. Scientists got together to make rules for working with recombinant DNA. They introduced ideas like biological containment that are still used today. The conference said that new scientific discoveries must be made with consideration of ethics. Over the few decades biosafety practices became more formalized.

The Biological Weapons Convention in 1975 made it illegal to develop, make or stockpile weapons. The Cartagena Protocol on Biosafety in 2000 defined biosafety in relation to biotechnology. The WHO's Laboratory Biosafety Manual, last revised in 2020 expanded biosafety to include all agents.

3.1.3 Contemporary Biosecurity Landscape

Biosafety governance used to focus on keeping laboratories safe. Now it also covers biotechnology, synthetic biology protecting the environment and preparing for global pandemics. With these advances the rules we have today were made before AI-assisted biological research became a thing. The first framework for assessing risks for AI use in synthetic biology was published in 2024.

3.2 Gain-of-Function Research in the Age of AI

3.2.1 What is Gain-of-Function Research?

Gain-of-function research is when scientists try to make pathogens stronger or more transmissible. They do this to understand how diseases work, predict how they might change and develop vaccines and treatments. Loss-of-function research is the opposite; it makes pathogens weaker. Often these two types of research overlap in the studies.

Between 2000 and 2022 researchers found around 7,000 publications that involved gain-of-function or loss-of-function methodologies worldwide. Researchers affiliated with the U.S. Contributed to half of these. This research happens at biosafety levels and uses various experimental approaches, including CRISPR-based gene editing.

3.2.2 Regulatory Challenges

The lines between gain-of-function and loss-of-function methodologies can blur, making it hard to restrict experiments without affecting less risky research. Researchers can't always predict if an experiment will make a pathogen more or less dangerous. What starts as low-risk work can unexpectedly become hazardous. The integration of AI into this field makes things both more possible and more risky.

AI systems can speed up analysis, predict protein structures and model pathogens, which can dramatically shorten research timelines. They can also make it easier for people to manipulate agents raising questions about who can access and use these capabilities.

4. Key Issues and Concerns

4.1. Biosecurity and Dual-Use AI in Biological Research

4.1.1 The Dual-Use Problem

As mentioned earlier AI can help produce vaccines, improve diagnostics and monitor diseases. However it also opens up ways to create pathogens. This problem has always existed in research but AI has made it easier and faster to develop dangerous biological agents.

The Centre for AI Safety says AI can cause harm in several ways. For example genetic sequences of viruses are available online. Modern AI technology can guide people in synthesizing pathogens even if they have knowledge. Protein design tools might create pathogens with properties of various agents.

4.1.2 AI in Synthetic Biology: Categories and Risks

In 2024 Applied Biosafety introduced a risk framework for AI in biology. The framework highlights the following risk categories:

- Gene editing guidance: risk of dual use because gene editing tools have widespread applicability.
- De novo engineering: extremely dangerous; AI can create new types of genetic combinations with unknown consequences.
- Alteration of genes sequence: possibility of misuse and unintended effects.
- Automated experiments in laboratory conditions: reduced human supervision increases the likelihood of misuse or error.
- Biological risk management tools: AI software that needs to be separated from dual-use considerations and supported.

Large language models like GPT-4 play no part in biological design tools but may provide suggestions to interpret outputs and assist in ways that affect biological safety.

4.1.3 Mitigation Strategies and Governance

Dual-use AI in sciences can be addressed both by technical and non-technical measures. There are two types of mitigation strategies:

- Pandemic-resilience strategies: enhanced air filtration, universal vaccines, monitoring of wastewater samples for pathogens and quick diagnostic kits.
- Prevention strategies: assessing usage patterns limiting access to AI models and DNA synthesising equipment and prohibiting the use of sensitive biological information in general-purpose AI models.

Governance must consider this aspect. A security-oriented approach to biosecurity as a part of scientists' professional duties is key to achieving biosecurity goals. Financial and educational requirements are tools to governments to encourage scientists to develop such an approach.

4.2 Algorithmic Bias and Accountability

4.2.1 Sources of Bias in Medical AI

A study published in PLOS Digital Health found that bias in medical AI systems can occur at any point in the development life cycle. Sources of bias include:

- Data collection: sample sizes of some demographic groups.
- Data labelling: biases from clinical experts.
- Model. Evaluation: overreliance on overall metrics.
- Deployment: performance in real-world settings.
- Publication: publication bias.

4.2.2 Clinical Consequences

AI in medicine results in misdiagnosis, inappropriate treatment and worse healthcare for marginalized communities. AI models exhibited sex, race and age biases during the COVID-19 pandemic. Simple recalibration measures can improve fairness.

Poor performance of tools for minority patients reduces institutional trust and aggravates existing inequalities.

4.2.3 Accountability Frameworks

Establishing liability in cases of use of medical AI technology is difficult due to unclear legal frameworks. Responsible parties might be AI developers, medical facilities or clinicians. No party being legally liable translates into patients suffering harm.

The IBM Watson for Oncology algorithm provided recommendations for some cancer treatments highlighting the need for better accountability mechanisms.

4.2.4 Approaches to Redress

Evidence-based measures include:

- Creating diverse datasets.
- Using debiasing techniques.
- Careful evaluation of subgroups.
- Making models explainable.
- Compulsory bias reporting.

Mandatory bias assessment before. After deployment is an important part of any regulatory process.

4.3 Ethical Limits of AI

4.3.1 Ethical Limits in Misdiagnosis

AI diagnostic errors can be traced to three interdependent failure modes, each demanding targeted mitigation. First, data pathology, driven by sampling biases, leads to systematic underdiagnosis in minority or underrepresented groups, as seen in elevated false-negative rates among dark-skinned patients. Second, algorithmic bias, often caused by overfitting to spurious patterns in training data, results in clinically significant false positives, such as unnecessary treatment for benign findings. Third, human-AI interaction issues, such as automation complacency or overreliance, can slow down error detection and correction, as demonstrated by delays in clinical workflows when AI is blindly trusted or ignored. The end-to-end AI diagnostic workflow, from data collection and model training to clinical application and iterative feedback, includes several points where technical flaws and systemic biases can be introduced and amplified.

Each stage represents a potential vulnerability, capable of propagating errors throughout the entire diagnostic process. The reliability and fairness of AI diagnostics rest on three pillars: data quality, diversity, algorithmic interpretability, and rigorous validation. High-quality, representative data are crucial to avoid systematic disadvantages for minorities. Complex models boost accuracy but may obscure reasoning, limiting clinicians' ability to verify diagnoses. Rigorous testing, including cross-validation on diverse datasets and real-world clinical trials, is essential to confirm safety and build

trust. While advanced deep learning models can surpass human experts in detecting subtle clinical patterns, their complexity often comes at the expense of interpretability.

The “black-box” nature of many models makes it difficult for clinicians to understand, verify, or challenge AI-generated diagnoses, eroding trust and increasing the risk of undetected errors. Techniques such as LIME and SHAP improve transparency, but typically offer only partial insights. Thorough external validation, including cross-validation across subgroups, and prospective real-world clinical trials, is critical for ensuring AI safety and reliability.

4.3.2 Epistemic Risks and Over-reliance on AI

Healthcare professionals emphasize that any new technology integrated into clinical practice must demonstrably support the delivery of high-quality patient care. A central requirement for the adoption of AI-based decision support systems (AI-DSS) is their reliability. This includes the ability to generate accurate, efficient, and personalized risk assessments, as well as evidence of robust clinical validation and transparent development processes. Clinicians particularly require confidence that such systems provide correct and actionable patient information to inform decisions, including critical judgments about when and how to intervene during care.

This expectation can be understood in terms of *epistemic reliance*, where a practitioner accepts a proposition as correct based on the output of a system. However, this differs from *epistemic trust*, which involves deeper normative and affective expectations toward the source of information.

In the context of medical AI, clinicians are less concerned with trusting the intentions or nature of the developers and more focused on whether the system produces reliable and clinically valid results. Importantly, clinicians do not accept the reliability of AI systems uncritically. Assessing the strengths, limitations, and appropriate applications of AI-DSS is considered part of their professional development responsibility to ensure safe and effective patient care.

Despite increasing integration of AI in healthcare, clinicians continue to regard their epistemic authority as central to clinical decision-making. Their expertise, experience, and access to contextual patient information position them as the final arbiters of care decisions. AI-DSS is therefore viewed as a supportive tool rather than a replacement for professional judgment.

Clinicians maintain responsibility, including legal and ethical accountability, for patient outcomes, and determine when and how AI outputs should influence decisions. While clinicians set a high threshold for incorporating AI tools into practice, these systems are not expected to be infallible. Instead, effective integration depends on a clear understanding of both the capabilities and limitations of AI-DSS.

Ultimately, clinicians seek systems that are reliable enough to inform decision-making while allowing them to retain interpretive control and responsibility within the clinical context.

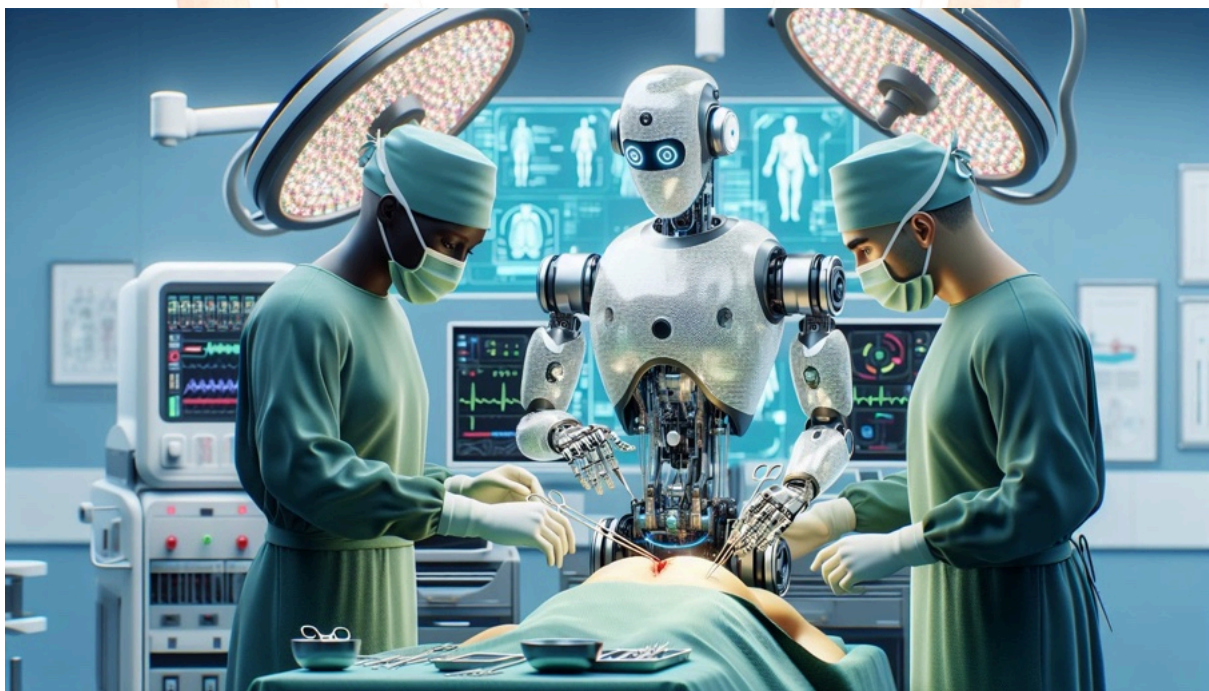
4.4 Transparency and Psychological Impact of AI in Healthcare

4.4.1 AI in Healthcare -

AI is being deeply integrated into AI and digital technology. From algorithms that screen X-rays and analyze genetic data, to mobile apps that triage symptoms or even chat with patients, AI systems promise to make medicine faster, cheaper, and more precise. In the context of pandemics like COVID-19, where AI tools were extensively used for rapid diagnosis, tracking, and treatment development, including AI-powered chest CT scan analysis.

It also reduces administrative burdens for staff, provides 24/7 patient monitoring via wearables, and improves surgical precision using robotics. These technologies enhance patient outcomes while addressing staff shortages. AI optimizes hospital workflows by automating administrative tasks (billing, scheduling) and reducing the time clinicians spend on electronic health records. Systems such as the Da Vinci robot increase precision, leading to less invasive procedures, fewer complications, and faster patient recovery.

However, these benefits raise new ethical concerns. AI algorithms rely on large datasets to "learn" and make predictions. In addition, they have enormous databases, which raises privacy concerns. If training data is inadequate or skewed, the system may produce incorrect diagnoses or biased suggestions, undermining patients' trust in doctors and healthcare systems. Along with that, AI medical tools require high costs to implement, and that may serve as a barrier for some healthcare institutions.



4.4.2 Psychological Impact

AI tools in healthcare create a mixed psychological impact, offering increased access, stigma reduction, and personalized care through apps like Headspace and Wysa. However, they also introduce anxiety regarding data privacy, depersonalization, and reduced human empathy.

The psychological impacts of incorrect decisions made by inaccurate AI medical models can be profound and enduring. A particularly distressing example is the erroneous prediction of a patient being diagnosed with a terminal illness, which can lead to tragic outcomes such as mistaken euthanasia. Such an event not only causes irreversible harm to the individual but also erodes the trust of patients and their families in healthcare institutions.

This loss of trust can contribute to long-term mental health issues, including depression and substantial regret, highlighting the necessity for accuracy and accountability in AI applications within medicine.

4.5 International Oversight, Transparency, and Regulatory Cooperation

4.5.1 Gaps in Existing Frameworks

Gaps in AI governance in biotechnology are numerous. The Biological Weapons Convention of 1975 provides a foundation but it does not cover AI. The International Health Regulations of 2005 set disease reporting requirements but have nothing to say about surveillance.

Currently there is no binding treaty regulating AI in biotechnological research or biosecurity.

4.5.2 Challenges to Accountability and Responsibility

The dispersal of responsibility among entities makes it difficult to assign accountability in cases of harm. Most legal systems lack guidelines for handling complicated multi-party decision making in AI technology applications.

4.5.3 Equity Access and Cross-Border Enforcement

The distribution of AI technology in medicine and biology is far from equitable. Countries with capacity for biomedical research have an advantage in terms of access to datasets and equipment. Any effort to restrict access to types of AI must be coordinated internationally. The need to identify users offer restricted access to hazardous technologies and avoid the shifting of hazardous activities to regions with weak oversight.

4.4.5 Moving Towards Proactive, Risk-Based Governance

Governance must always be proactive, rather than reactive. A framework of risk assessment based on vulnerability assessment consequence analysis and risk level determination allows for assessment of AI tools before releasing them. The adoption of this standard would oblige developers to undertake biosecurity assessment before launching products.



5. International Standards and Framework

The rapid growth of artificial intelligence in biological research and healthcare is moving faster than the creation of international regulations. There are several global frameworks in bioethics and public health, but they were developed before AI-driven systems emerged. Existing governance frameworks are not able to fully address the ethical, technical, and security issues that AI biological applications present.

Here, we discuss current frameworks, their relevance, and critical gaps that need attention to ensure the safe, fair, and ethical use of AI in biosecurity and healthcare.

5.1 Existing Bioethics Frameworks

Bioethics has been the foundation for ethics in medicine and biology for many years. The principles of autonomy, beneficence, non-maleficence, and justice are essential in ensuring that people receive ethical treatment as science advances.

At the international level, an important framework is the Universal Declaration on Bioethics and Human Rights from UNESCO. It highlights the importance of informed consent, human dignity, and equal treatment for all in healthcare. Similarly, ethical guidelines from the World Health Organization focus on patient well-being, fairness, and public health.

However, these frameworks have worked well when humans made decisions in medicine. They have limitations when it comes to AI technology.

The Challenge of Machine-Assisted Decision-Making

AI systems are increasingly used for diagnosing diseases, suggesting treatments, and predicting health outcomes. While they can analyze data faster and sometimes more accurately than humans, they often operate as “black boxes.” Even experts may not fully understand how they reach their conclusions.

This creates a conflict with the principle of informed consent. If a patient cannot grasp how a diagnosis is made, their ability to make informed choices is restricted. This raises a key ethical question: should decisions that impact human lives rely on systems that are not fully understandable?

5.1.1 Accountability within an AI-Based Framework

Bioethics operates under the assumption that accountability is well-defined. Yet, the introduction of AI into the process raises questions. In the case of a medical malpractice that involved the use of an AI system, the following could be considered responsible: Developers of the software algorithm, entities that implemented the algorithm, and medical practitioners who utilized it. These multiple levels of accountability make it difficult to determine accountability, leading to ambiguity and injustice.

A real-world example can be: IBM Watson for Oncology was found to recommend dangerous treatments in certain cases, sparking debate about data ethics and consent.

AI systems depend on large amounts of data, frequently involving health and genetic data. While current guidelines focus on consent, they overlook other aspects of data usage, including: Secondary use of data, Data transfer across borders, and Storage of data.

Case Study Analysis:

Google DeepMind's acquisition of patient data from the NHS in the United Kingdom without consent led to a backlash. This demonstrates that ethical considerations can be easily overlooked in the quest for technological advancement.



5.1.2 AI Ethics, and Consent

The use of AI technology is significantly dependent upon big data that includes personal, genetic, and medical data. While there is a framework currently developed in light of the issue of consent, this framework fails to recognize the evolving dynamics of how data is handled, including:

- Data reuse
- Cross-border transfer of data
- Data storage and reuse

Case Study Insights: Google DeepMind in the UK faced criticism for accessing personal patient data without consent from the NHS

5.1.3 Influence on Human Beings and Psychological Considerations

AI technology employed in healthcare can significantly influence human lives. The situation is particularly alarming when people receive their diagnoses from algorithms.

Patients may experience:

- Anxiety
- Overdependence on technological solutions
- Loss of faith in healthcare professionals

This problem is usually ignored in standard approaches to bioethics.

5.1.4 Complex Questions Regarding Life and Death

One of the most difficult ethical considerations concerns AI technologies' involvement in euthanasia and end-of-life healthcare. Although the current theoretical frameworks focus on mercy and human consideration, there are other issues to consider: Is it possible for an algorithm to understand, and human pain?

Should AI advice be taken into account regarding life and death matters?

How to accommodate cultural and ethical diversities?

These questions still lack proper answers in today's frameworks.

5.1.5 Existing Bioethics Frameworks

UNESCO's Universal Declaration on Bioethics and Human Rights (2005)

An important international framework governing bioethical issues is the Universal Declaration on Bioethics and Human Rights adopted by UNESCO in 2005. The declaration establishes key principles including human dignity, informed consent, privacy, equality, justice, and respect for cultural diversity. It emphasizes that scientific and technological advancements should always prioritize human welfare and fundamental rights. Although the declaration was created before the widespread adoption of artificial intelligence in healthcare, many of its principles remain highly relevant today.

Issues such as algorithmic bias, patient privacy, and AI-assisted medical decision-making can be evaluated through the framework's emphasis on human dignity and individual rights.

5.1.6 WHO Guidance on Artificial Intelligence in Health

Recognizing the growing role of AI in healthcare, the World Health Organization published guidance on the Ethics and Governance of Artificial Intelligence for Health in 2021. The guidance outlines six key principles:

- Protection of human autonomy
- Promotion of human well-being and safety
- Transparency and explainability
- Accountability and responsibility
- Inclusiveness and equity
- Sustainable and responsive AI systems

The WHO stresses that AI should support rather than replace human decision-making and that sufficient human oversight must remain present in all healthcare applications.

5.2 Global Health Governance and Policies

The system of global health governance is based on the idea of cooperation among countries through institutions such as WHO. The International Health Regulations (IHR), which are one of the international health policies, aim to ensure coordinated responses to health problems around the globe.

5.2.1 Role of AI in Modern Health Governance

AI implementation in the field of global health is posing some challenges. A. Role of AI in Modern Health Governance. The use of AI technologies is increasingly becoming common in modern health governance, especially in aspects such as:

- Disease monitoring and outbreak forecasting
- Diagnosis and imaging support
- Health resource distribution and planning
- Pharmaceutical research

While their application has proven highly efficient, these technological developments have also created new health governance concerns.

5.2.2 Accountability in AI

Bioethics depends on accountability and traceable lines of responsibility of individuals or institutions involved in making certain medical decisions. In the case of artificial intelligence, the responsibility for making certain decisions gets spread across several stakeholders.

In the case of a mistake resulting from an artificial intelligence algorithm—be it a misdiagnosis or an incorrect treatment—the following individuals might be responsible:

Algorithm developers

Data providers who offer biased data

Healthcare institutions that use this algorithm

Doctors who rely on the results provided by the system

It makes tracing responsibilities even harder, while mistakes can come due to any of these aspects. Another problem associated with artificial intelligence is automation bias. Many times, professionals might have too much faith in the algorithms used.

Another issue concerns the transparency of artificial intelligence programs. It may be challenging to explain some decisions.

5.2.3 Disparity in the Availability of AI Technologies

The advantages of AI technology in the fields of medicine and biological sciences are not equally distributed across the globe. The leading nations in AI development include those that have better technological capacity, more funding, access to research institutions, and highly skilled professionals. On the other hand, underdeveloped countries still experience difficulties such as insufficient finances, technical knowledge, and information infrastructures. Such disparities will eventually result in growing inequalities between different regions, limit availability to technological medicine, and create dependency on technologically developed countries for healthcare equipment.

5.2.4 Bias and Discrimination

Access to AI technologies is unevenly distributed throughout the globe. While developed nations hold an advantage over others in terms of research and development related to AI, as well as infrastructures that allow such technologies, these nations have an upper hand over those in less advanced regions when it comes to advancements in AI-based health care and biological research. Developing countries may struggle to develop health care technology and research due to their financial limitations and lack of proper technology and data infrastructures.

5.2.5 Ethical Dilemmas in Sensitive Applications

Firstly, there exist many instances where the application of AI in medicine and biosciences has not been subject to international regulation. These include mental support systems developed using AI, genetic testing tools, as well as decisions about end-of-life care that are made with the assistance of AI, creating serious ethical questions in terms of privacy, consent, emotional balance, and human dignity, respectively. On the other hand, the application of AI could impact highly personal decisions due to its inability to fully grasp all cultural, emotional, and moral implications of certain healthcare situations.

Secondly, there is no common understanding regarding euthanasia, genetic modification, and mental health among countries due to the legal, cultural, and religious differences existing among them.

5.2.6 Psychological and Social Threats

Apart from posing risks to the patient's safety and security, the rise of artificial intelligence in the field of medicine has brought about several psychological and social risks. While AI technologies may contribute to increased accessibility, efficiency, and provision of early assistance, heavy reliance on technological innovations might lower human engagement in the healthcare environment, which, in turn, may undermine trust in healthcare professionals.

In addition, patients may come to rely greatly on AI systems for their emotional comfort and medical help, especially when dealing with sensitive issues, including mental well-being and chronic disorders.

It may also be difficult for an AI system to comprehend human emotions, cultural nuances, and mental problems.

Case Study Implication:

Woebot is among the many mental health applications that have made mental health counseling more affordable and accessible to people. Nevertheless, there are issues related to emotional dependency on the AI system, incorrect medical advice, and a lack of professional supervision, especially when addressing severe psychological problems.

5.2.7 Biological Weapons Convention (BWC)

One of the most important international agreements related to biosecurity is the Biological Weapons Convention, which entered into force in 1975. The Convention prohibits the development, production, stockpiling, and acquisition of biological weapons.

Although the BWC was drafted decades before artificial intelligence became a major scientific tool, its objectives remain highly relevant. AI technologies are increasingly being used in synthetic biology, pathogen research, and genetic engineering. While these technologies offer substantial benefits for medicine and public health, they also create concerns regarding dual-use research, where scientific advances intended for beneficial purposes could potentially be exploited for harmful applications.

Many experts have therefore called for discussions regarding how the BWC can be adapted to address AI-assisted biological research and emerging biosecurity risks.

5.3 Shortcomings in Regulatory Frameworks

In spite of the availability of international bioethics principles and global health guidelines, considerable shortcomings still exist within the regulatory frameworks for artificial intelligence-based biological systems. The existing regulations have been formulated before the fast emergence of artificial intelligence technology, and thus lack an effective mechanism for addressing some of the ethical, legal, and security issues that have emerged in relation to the use of this technology.

5.3.1 Lack of International Treaty on Biosecurity Related to Artificial Intelligence

The first problem in regulation that requires addressing is the lack of an international treaty governing the use of artificial intelligence in the field of biotechnological studies and biosecurity. In fact, although there are numerous documents related to biotechnology, human health, and welfare, only a few address the issue of utilizing AI technology in the field.

However, this problem needs to be addressed due to the fact that the majority of biotechnological advances developed using artificial intelligence technology possess a dual nature. In other words, the same tools used to advance scientific knowledge and facilitate medical research can be employed for creating and deploying dangerous biological agents, and even conducting bioterrorism.

What is more, since the rate of technological advancements outpaces the policy-making process, many nations are not able to develop sufficient regulation regarding the use of highly sophisticated AI systems in biotech laboratories.

5.3.2 Uncertainty Relating to the Structure of Liability

One more critical case of regulatory failure is related to the absence of a structure of liability that would help define the responsibilities following the occurrence of harmful effects due to using artificial intelligence. Should medical professionals err in their work because of the application of artificial intelligence technology, carry out faulty research, or demonstrate discriminatory behaviors when working with patients, there is no specific mechanism to prove liability in such cases.

It results in many uncertainties about which entity would be responsible, and how to act legally in such circumstances. Sometimes, the legislation fails to offer any rules concerning complicated decision-making procedures that occur because of using new technologies. In the face of greater involvement of artificial intelligence in medical practices and biological research, such an issue should be resolved as soon as possible.

5.3.3 Auditability and Liability Mechanisms

As AI becomes more integrated into healthcare systems, experts increasingly emphasize the need for auditability. Auditability refers to the ability to trace how an AI system arrived at a particular conclusion or recommendation.

Regular independent audits can help identify biases, technical flaws, security vulnerabilities, and regulatory violations before they cause harm. Such mechanisms also improve transparency and public confidence in AI technologies.

In addition, many legal scholars advocate for clearer liability frameworks that define the responsibilities of developers, healthcare institutions, governments, and medical professionals. Without clearly established liability structures, individuals harmed by AI-related errors may face difficulties seeking accountability or compensation.

5.3.4 Bias and Discrimination

Bias and discrimination are still some of the most important challenges associated with the implementation of AI systems, especially within the sphere of medicine and biological research. The performance of AI systems is significantly determined by their training sets. When the datasets are incomplete, skewed, or reflect pre-existing social disparities, the results generated by the AI system could be biased as well.

This may lead to unfair healthcare recommendations or diagnostics that are not appropriate for certain groups of people due to racial, gender, economic, or geographical differences. In many instances, there is no universal control framework that would make sure that AI is used

fairly, transparently, and inclusively. Therefore, the development of biased algorithms could remain uncontrolled, and unfair practices will be promoted.

5.3.5 Ethical Uncertainty with Regard to Sensory Applications

There are a number of areas where the use of AI in medicine or biological studies has not been regulated by international law. Examples include the application of AI in mental healthcare facilities, genetic testing equipment, and end-of-life decisions that can include euthanasia, and recommendations regarding the use of life support technology.

While mental healthcare systems that are powered by AI may be useful in terms of availability, the emotional dependencies created by such technology, as well as the lack of oversight in such situations, can prove to be problematic in ethical terms. Similarly, while early detection of disease via genetic testing through AI systems can be useful, there is a risk of discrimination based on such genetic tests.

The topic of end-of-life decisions is perhaps the most controversial one, as different nations have their own cultural, legal, and religious views when it comes to such practices as euthanasia and the use of life support systems.

5.3.6 Data Privacy and Cross-Border Data Protection

A growing concern in AI-driven healthcare is the protection of sensitive medical and genetic information. Many AI systems rely on large datasets collected from multiple countries and institutions. However, regulations governing the transfer and use of such data vary significantly across jurisdictions.

Questions regarding data ownership, patient consent, cybersecurity, and international data sharing remain unresolved. The absence of harmonized global standards increases the risk of privacy violations, unauthorized access, and misuse of sensitive biological information.

The controversy surrounding Google DeepMind's use of NHS patient data demonstrates the challenges of balancing innovation with privacy protection in modern healthcare systems.

5.3.7 Psychological and Social Issues

The rising popularity of artificial intelligence in medicine has generated other critical psychological and social issues. Although AI applications enhance accessibility and speed up support delivery, an overreliance on technological solutions could lead to a lack of human contact in healthcare environments and erode patients' confidence in their medical practitioners. Patients could develop psychological dependence on artificial intelligence programs, particularly for sensitive issues such as mental well-being services.

Case Study Analysis: Artificial intelligence-powered mental wellness apps like Woebot have improved access to mental well-being help services. Nevertheless, there are worries about emotional dependency, incorrect feedback, and a lack of medical supervision in serious psychological disorders.

- Possibility of its further distribution

There was also the problem associated with the participation of private companies in the work of national healthcare facilities. Some researchers were concerned about the possibility of commercial exploitation of sensitive patient data and the extent of potential corporate involvement in healthcare infrastructure development.

Finally, the case proved that current legislation may be inadequate when regulating advanced data-driven healthcare systems incorporating machine learning technologies.

5.3.8 Conclusion of Case Studies

As the presented case studies demonstrate, the challenges discussed during this presentation have a significant impact on the lives of people all around the world. While the use of AI promises many benefits to health care systems and science in general, its unregulated development and application may result in discrimination, abuse, unequal treatment, and violation of individual rights.

In addition to technological advancements, there is also a need for proper governance and regulation to prevent the misuse of AI in the field under discussion.

For this reason, delegates should be aware of real-world examples that show negative effects associated with the lack of regulation in practice.

6. Stakeholder Analysis

In biosecurity, stakeholders are identified through their involvement and impact in the training, testing, and implementation of AI systems used in disease detection. These include individuals and groups who share expert insights and knowledge, participate in interviews, and are involved in real-life applications of such algorithms. Their role is crucial in understanding how these AI systems function, including their usefulness, the challenges they face, and ethical concerns. Stakeholders are also connected to areas like public health surveillance, showing that biosecurity is not only a technical field but one shaped by the input and decisions of multiple actors. Addressing biosecurity challenges requires the participation of these stakeholders, including governments, healthcare institutions, artificial intelligence creators, tech companies, media, and civil society organisations, all of whom play a key role in different parts of biosecurity.

6.1 Governments

Governments are pivotal stakeholders in biosecurity as they are responsible for detecting, reporting, and responding to disease outbreaks through public health institutions. They play an essential role in disease monitoring by collecting and analysing medical data from healthcare providers and laboratories. Governments also work with international partners to monitor or control the spread of harmful diseases and share information to strengthen early warning systems. In addition, they support medical research aimed at improving diagnostic methods and understanding diseases, which strengthens detection capabilities. Governments are the primary stakeholders involved in preparing for and managing large-scale health emergencies like pandemics, and in coordinating responses across health institutions. At the international level, governments are the architects and enforcers of multilateral biosecurity frameworks, including the Biological Weapons Convention (BWC). However, existing frameworks such as the BWC predate the AI era and were not designed to address the specific risks posed by algorithmic tools. As CAIS notes, effective governance requires helping the scientific community adopt a security mindset, a cultural shift that governments can promote through funding, regulation, and the embedding of security education in research training programmes. A particular governance challenge is that AI capabilities are advancing faster than regulatory frameworks can evolve. CAIS calls for developing specific regulations and best practices, updated regularly, and for transparent measurement of security effectiveness in practice, including red-teaming of DNA synthesis services and AI models, as core responsibilities of government bodies.

6.2 Healthcare Institutions

Healthcare institutions like hospitals, laboratories, public health institutes, and research institutes work towards finding treatments for disease outbreaks and providing crucial health services during emergencies. They are essential in disease monitoring. They deal with patients at the primary level, identify their cases, and then report medical data to public health authorities and laboratories for further monitoring and response. Hospitals and laboratories help in the early detection of infectious diseases, allowing for quicker identification of outbreaks and biological threats. Healthcare institutions and their affiliates support medical research during health emergencies by constantly studying and monitoring developments, which is the most important aspect of finding a cure. Clinical laboratories further play a critical role in confirming diseases by testing and generating accurate data that aids in decisions related to an outbreak. Healthcare facilities are also involved in implementing disease prevention and control measures. Moreover, healthcare institutions work with national and international health agencies to prepare for potential outbreaks and pandemics.

In view of AI bias, healthcare institutions are also the main places where biased AI systems cause patients direct harm. The AI models' performance can deteriorate when they are deployed outside the environment in which they were trained, and they do so unequally across different patient subgroups. This means that healthcare institutions have a responsibility to not only implement AI systems, but also monitor their real-world performance, report bias incidents, and maintain strong clinical oversight so that AI models are always supervised by qualified human practitioners.

6.3 AI Developers and Tech Companies

AI developers and technology companies are the ones who create the AI algorithms used in disease detection, diagnosis, and gain-of-function research. It is their responsibility to make sure that these systems are safe, reliable, and transparent when used in the medical field. Developers also need to reduce AI bias and ensure fairness, as highlighted in international AI principles. Before these AI systems are used on patients or for research, they must be properly tested and approved. Technology companies work with hospitals and governments to improve disease detection in AI models by using large amounts of medical data. This helps in the early detection of diseases. By developing new tools that make treatments faster and more accurate, these companies also support medical innovation. At the same time, they must follow ethical guidelines to protect each patient's data.



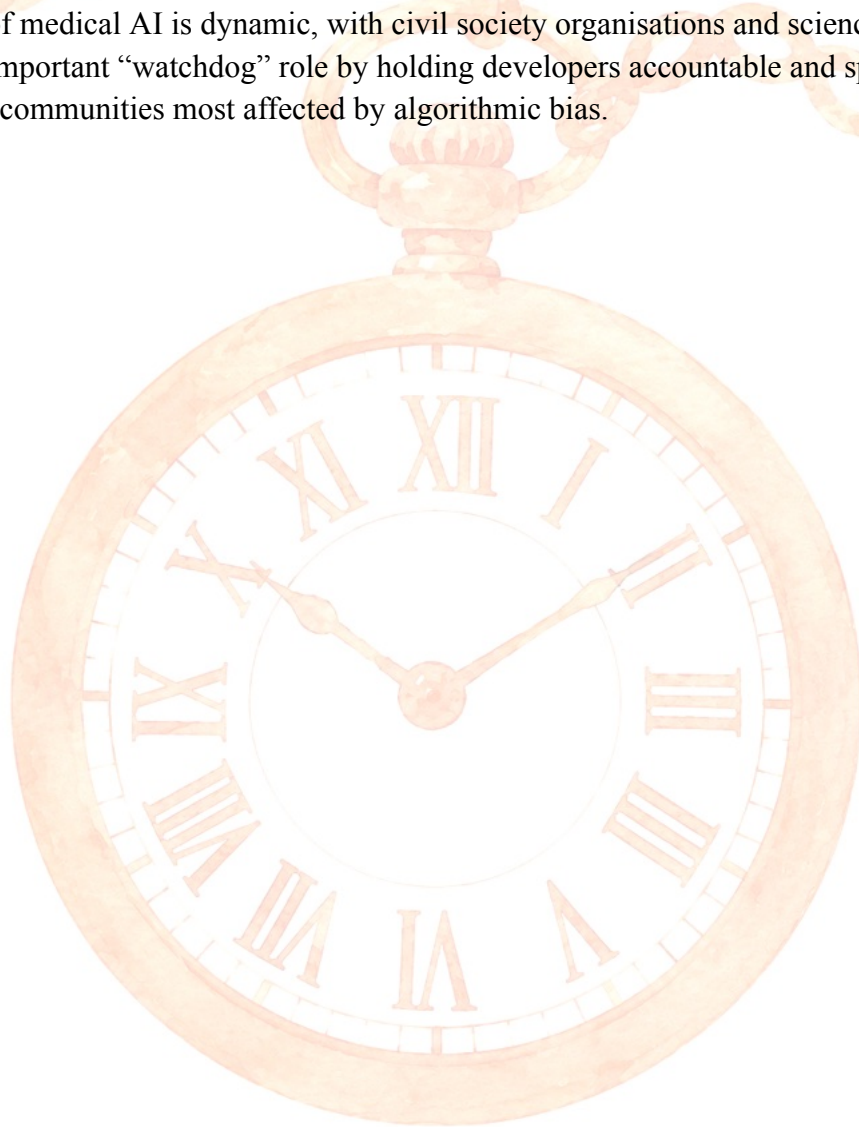
On the biosecurity side, CAIS emphasises that AI developers bear a specific responsibility to exclude certain categories of biological knowledge from widely accessible AI systems, so as to prevent them from coaching malicious actors through the creation of a virus. Access to AIs with hazardous biological knowledge should be restricted to vetted researchers. Developers must also conduct evaluations and red-teaming to prevent the release of AI models that can assist with the synthesis and release of pathogens. The open-source release of powerful biological AI tools presents a particular challenge: when models with dual-use potential are made freely available, the ability of developers to control downstream use is substantially diminished. AI developers and biorisk management professionals can systematically identify, evaluate, and mitigate the biosecurity risks of AI tools used in synthetic biology. This is an approach that delegates may wish to refer to when designing governance provisions for AI developers.

6.4 Civil Society and Media

According to UNESCO, civil society refers to the collective of non-governmental organisations, community groups, and associations that operate independently of the state and the market. As an important stakeholder, civil society consists of NGOs, communities, and individuals who help spread awareness and support action taken against biological threats. It is recognised that governments alone cannot manage biosecurity risks, and there must be cooperation between official governmental policies and community-level efforts to deal with issues like disease outbreaks. Civil society raises awareness about the risks and misuse of biological research and experiments, which is important for preventing mishaps. Research shows that public participation and social awareness are important in responding to global health emergencies and improving how people handle disease outbreaks.

The media is the stakeholder that shares information between authorities and the public during outbreaks, helping people to understand what is happening, what risks they face, and what actions they should take to stay safe. Good communication through the media is very important. If information is unclear or delayed, it can slow down disease control and reduce public trust. Spreading important health advice, such as hygiene practices, avoiding infected areas, and reporting symptoms, helps in controlling the spread of diseases. However, it is important that the media reports responsibly and avoids spreading misinformation or panic. Wrong information can make people afraid to report symptoms or follow health guidelines. By encouraging responsible behaviour and effective communication during disease outbreaks, the media helps civil society in carrying out its tasks during a global health crisis.

The future of medical AI is dynamic, with civil society organisations and science journalists playing an important “watchdog” role by holding developers accountable and spreading the concerns of communities most affected by algorithmic bias.



7. Challenges and Limitations

There are a number of notable challenges and limitations in the application of artificial intelligence to bioethics and the detection of diseases. First of all, there is the problem of accessing good-quality data, as medical data is limited, incomplete, or restricted due to data protection. Besides, AI requires large sets of data that should be collected over a long period and involve a lot of human work. The fact that AI systems are tested only in a laboratory setting may cause them to function poorly in the real world and fail to operate correctly when applied to other people or situations. Delegates also need to address the problems of bias, lack of transparency, and AI ethics in the committee.

7.1 Technological Constraints

7.1.1 Data Quality, Diversity, and Availability

Insufficient sample sizes for certain patient groups are a root cause of biased and unreliable AI in medicine. Medical data is often siloed within individual institutions, incomplete, inconsistently formatted, and subject to strict privacy regulations that limit sharing. Building the large, diverse datasets required to train unbiased diagnostic AI is, therefore, technically and institutionally challenging. Missing data that is nonrandomly absent, for example, diagnosis codes recorded less frequently for marginalised patients due to lower healthcare access, further distorts models trained on such data. Social determinants of health, which are rarely captured in structured medical records, represent a particularly significant gap.

7.1.2 Model Interpretability and the Black-Box Problem

Overreliance on other performance metrics during model development may obscure bias and diminish a model's clinical utility. Many high-performing AI systems operate as 'black boxes' whose internal reasoning cannot easily be questioned. This limits error traceability, undermines clinician trust, and makes it difficult to determine when or why a model produces biased or incorrect outputs. Emphasising model interpretability is one of the solutions the authors identify. Still, there is often a trade-off between predictive accuracy and interpretability that the field has not yet fully resolved.

7.1.3 Real-World Deployment vs. Laboratory Validation

A challenge documented many times is the gap between AI performance in controlled settings and its performance in real-world environments. When AI models are applied to data outside the training cohort, performance can deteriorate, meaning that a model validated as accurately as possible may perform substantially worse for underrepresented patients in practice. This clearly shows the importance of rigorous clinical trial validation before deployment and of ongoing post-deployment surveillance.

7.1.4 The Pace of Technological Change

CAIS notes that AI capabilities are advancing in ways that outpace existing governance and regulatory frameworks. The analysis of gain-of-function research provides a clear example: if a virus might plausibly be easy to synthesise using equipment available ten years from now, then unrestricted publication of its genome today could be considered high risk, yet existing regulatory frameworks rarely account for anticipated technological trajectories. Restrictions, CAIS argues, must be applied before the first cases of an engineered virus become visible, because by then it will be too late to head off the resulting pandemic.

7.2 Ethical Dilemmas

7.2.1 Dual Use and the Limits of Openness

The dual-use dilemma sits at the heart of this committee's agenda. The publishing of research freely, sharing data, and building on the work of others, is in direct tension with the biosecurity imperative to restrict access to knowledge that could be weaponised. CAIS acknowledges that this is never easy: virology is already under a heavy regulatory burden, and adding to it should not be taken lightly. Yet the stakes are now higher than ever before. The impact of a new AI-engineered pandemic could be vastly greater than that of an improperly approved drug. Norms need to adapt to changing circumstances, even when such adaptation is difficult.

7.2.2 Bias, Equity, and the Ethics of AI in Healthcare

Addressing biases across all stages of model development is a moral imperative. If it is left unaddressed, biased medical AI can worsen medical disparities, delivering worse care to already marginalised populations. The ethical obligation of developers, healthcare institutions, and regulators is therefore not satisfied by demonstrating that an AI performs well on average; it requires demonstrating equal performance across demographic subgroups. The committee should consider what standards are appropriate, what disclosure obligations are necessary, and what accountability mechanisms are needed when these standards are not met.

7.2.3 Informed Consent and Transparency

An underexplored ethical dimension of AI in healthcare is informed consent. When AI systems influence diagnosis or treatment decisions, patients have a reasonable interest in knowing that such tools are being used, how they work, and what their limitations are. The opacity of many AI systems makes meaningful informed consent difficult to apply. Delegates should consider whether transparency requirements for AI in healthcare, analogous to requirements for disclosure of clinical trial information, are an appropriate policy response.

7.2.4 The Governance Gap and International Responsibility

CAIS frames the governance challenge bluntly: the important question is whether we succeed in preventing an engineered pandemic, not merely whether we comply with regulations. This reframing has significant implications. It suggests that the adequacy of governance frameworks must be measured by outcomes, actual security achieved, not by procedural compliance. For a multilateral body like this committee, the challenge is to design international standards that are ambitious enough to close real security gaps while being operationally feasible across countries with very different regulatory capacities and scientific cultures.

7.3 Legal and Regulatory Barriers

7.3.1 Outdated Frameworks

Existing legal instruments governing biological research and AI were not designed with the current threat landscape in mind. The Biological Weapons Convention predates the era of AI-assisted synthetic biology. Most AI regulatory frameworks do not include specific provisions for dual-use biological AI. Medical device regulations in many jurisdictions do not require pre-market testing for algorithmic bias across demographic subgroups. Although there are many AI risk assessment frameworks in the literature, and risk assessment frameworks for synthetic biology, the first specific risk assessment framework for the use of AI in synthetic biology was published only in 2024, highlighting how recently the field has begun to grapple with this intersection.

7.3.2 Cross-Border Enforcement

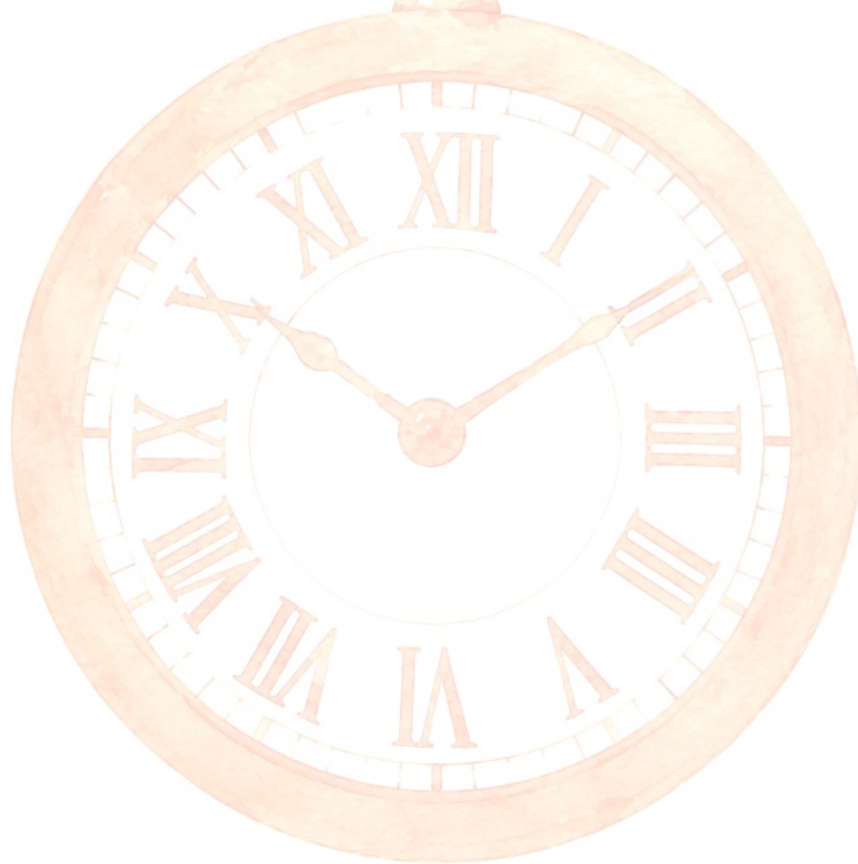
AI development and deployment are inherently global, but legal authority remains primarily national. As CAIS highlights, any restrictions on access to dangerous AI or biological knowledge must be effective in practice, not merely on paper. Maintaining effective restrictions requires new international coordination mechanisms, identifying legitimate researchers, providing them with vetted access, and preventing the relocation of high-risk research to lower-oversight jurisdictions. These are institutional and political challenges as much as technical ones.

7.3.3 The Need for Proactive, Risk-Based Governance

Both CAIS and De Haro emphasise that governance must be proactive rather than reactive. For AI in synthetic biology, De Haro proposes a structured risk assessment process, using tools such as vulnerability identification, consequence analysis, and risk-level determination, that enables biorisk management professionals to systematically evaluate and mitigate risks before they materialise. This risk-based approach, if adopted as a regulatory standard, could require AI developers to demonstrate that their tools have been assessed for biosecurity implications before release: a significant but arguably necessary shift in the current regulatory posture.

Standardised bias reporting and transparency requirements and rigorous clinical trial validation before real-world implementation are also called for.

Together, these recommendations from the primary literature point toward a governance model centred on prior assessment, transparency, ongoing monitoring, and clear accountability — principles that delegates should seek to embed in any resolution they draft.



8. Case Studies

8.1 United Kingdom – The Royal Free NHS Trust and DeepMind Data Scandal

The collaboration between the Royal Free NHS Trust and the tech company DeepMind in the UK became one of the first controversial episodes where questions arose about AI, healthcare policy, and data privacy in patients. Initially, the Royal Free NHS Trust joined hands with DeepMind in 2015 to create an application, known as "Streams," aimed at identifying people who had high risks of suffering from acute kidney injury with the help of the rapid electronic processing of health records. According to sources, acute kidney injury leads to thousands of fatalities in the country each year. Therefore, the project appeared to be an innovative attempt to enhance healthcare system efficiency by employing artificial intelligence.

However, the project soon became subject to intense scrutiny due to evidence that the confidential health information of about 1.6 million patients had been passed on to DeepMind without proper consent from the patients concerned. Most of the patients did not have any prior history of kidney disease, nor were they aware that their data was being used and processed by a private technology company. In 2017, the UK Information Commissioner's Office determined that the arrangement between Royal Free London NHS Foundation Trust and DeepMind Health was in violation of British data protection laws, since patients had not been provided with sufficient information on how their data would be stored and processed.

As a result of this scandal, debates erupted across Europe on issues surrounding medical privacy, the role of corporations in healthcare infrastructure, and the ethics involved with AI-assisted medicine. It was claimed that healthcare organizations had begun focusing more on technology rather than patient rights and transparency. Other concerns raised included the risk that healthcare data could one day be commodified if proper regulations were not implemented. There is an evident gap in regulation as the technology behind AI-driven medicine is advancing much faster than the ethical and legal frameworks intended to control it.

8.2 Netherlands and Belgium – Predictive AI and the Euthanasia Debate

The Netherlands and Belgium have emerged as central examples in global discussions surrounding predictive artificial intelligence, healthcare ethics, and euthanasia. Both countries legally permit euthanasia under specific legal and medical conditions and have increasingly explored the use of AI-assisted healthcare systems capable of predicting disease progression, estimating mortality risks, and recommending palliative care strategies.

These developments have become particularly significant due to demographic pressures caused by aging populations. In the Netherlands, nearly 20% of the population is above the age of 65, placing increasing strain on healthcare systems and long-term care services. Supporters of predictive AI technologies argue that such systems can improve medical efficiency, support doctors in identifying high-risk patients earlier, and reduce unnecessary suffering by assisting in treatment planning and end-of-life care decisions.

However, critics fear that predictive healthcare technologies may fundamentally alter societal attitudes toward illness, disability, aging, and medical dignity. Bioethicists have warned that AI-generated mortality predictions could unintentionally influence euthanasia-related decisions by shaping perceptions regarding quality of life, survival probability, and the allocation of limited healthcare resources. Concerns have also emerged that patients informed of poor algorithmic survival predictions may experience psychological distress, hopelessness, or subtle pressure toward accepting end-of-life care options.

These debates intensified during the COVID-19 pandemic, when hospitals across Europe faced severe shortages of intensive care beds, ventilators, and medical personnel. Questions arose regarding whether predictive algorithms could contribute to discriminatory triage systems that prioritize healthcare access based on age, disability, or projected survival outcomes rather than individual dignity and medical judgment.

8.3 Israel – Counterterrorism Surveillance Technology Used for Pandemic Monitoring

During the COVID-19 pandemic, Israel became one of the first countries to repurpose national security surveillance infrastructure for civilian public health monitoring. In 2020, the Israeli government authorized the Shin Bet security agency to use counterterrorism technologies originally designed to track suspected militants to monitor individuals exposed to COVID-19. The surveillance program utilized smartphone location data, movement histories, and digital tracking systems to identify potential contacts of infected individuals and support outbreak containment efforts.

Israeli authorities defended the program by arguing that the extraordinary nature of the pandemic required rapid and technologically advanced responses capable of identifying infection chains more efficiently than traditional contact tracing methods. Supporters claimed that the use of digital surveillance strengthened public health management and allowed authorities to respond quickly during a rapidly escalating global crisis.

However, the decision generated widespread criticism from civil liberties organizations, legal experts, and privacy advocates. Critics argued that the government had blurred the boundary between national security operations and civilian healthcare governance by deploying intelligence surveillance technologies against the general population. Concerns emerged regarding the absence of meaningful public consent, limited parliamentary oversight, and the long-term implications of normalizing emergency surveillance measures.

The controversy intensified when fears arose that surveillance systems introduced during the pandemic could remain operational even after the immediate health emergency ended. In response, the Israeli Supreme Court ruled that parts of the program required stronger legal supervision and greater legislative oversight.

8.4 China – The He Jiankui CRISPR Experiment and Global Biosafety Concerns

In 2018, Chinese scientist He Jiankui announced that he had successfully created the world's first genetically edited babies using CRISPR-Cas9 gene-editing technology. According to his claims, the embryos were genetically modified before birth to provide resistance against HIV infection. The announcement immediately triggered global outrage from scientists, governments, and bioethicists, many of whom condemned the experiment as unethical, reckless, and dangerously premature.

The controversy extended far beyond questions of medical ethics. Investigations later suggested that ethical approval procedures had been manipulated and that participants may not have fully understood the long-term risks associated with the experiment. Chinese authorities ultimately sentenced He Jiankui to prison for conducting illegal medical practices.

The incident exposed major weaknesses within international biosafety governance systems and demonstrated how rapidly advancing biotechnology can outpace existing regulatory frameworks. Although genetic engineering technologies continue to develop rapidly, there remains no universally enforceable international mechanism capable of effectively regulating or monitoring high-risk human genetic experimentation.

The case also intensified concerns regarding the growing intersection between artificial intelligence and biotechnology. AI systems are increasingly used in genomic sequencing, protein prediction, and genetic engineering research, allowing scientists to accelerate biological experimentation at unprecedented speeds. While these technologies may support medical innovation and disease prevention, experts warn that they could also facilitate dangerous genetic manipulation, engineered biological agents, or unauthorized human experimentation if left insufficiently regulated.

8.5 Russia – The Sverdlovsk Anthrax Leak and Modern Biosecurity Risks

One of the most serious biosafety disasters in modern history occurred in 1979 in the Soviet city of Sverdlovsk, now known as Yekaterinburg, where anthrax spores were accidentally released from a covert military biological research facility. The airborne release exposed nearby civilians to anthrax, causing at least 66 confirmed deaths, although several investigations suggest that the actual number of casualties may have been significantly higher.

For years, Soviet authorities denied responsibility and falsely attributed the outbreak to contaminated meat. Only after the collapse of the Soviet Union did investigations confirm

that the incident originated from Compound 19, a secret biological weapons laboratory involved in military biowarfare research.

The Sverdlovsk anthrax leak became one of the most significant historical examples of how secrecy, weak oversight, and a lack of transparency can intensify public health disasters. The Soviet government's efforts to conceal the true cause of the outbreak delayed medical responses, obstructed international investigations, and prevented accurate public awareness regarding the scale of exposure.

Although the incident occurred decades before the rise of artificial intelligence, it remains highly relevant to modern debates surrounding AI-assisted biotechnology and biosecurity governance. Today, AI systems are increasingly integrated into pathogen modeling, genomic sequencing, synthetic biology, and pharmaceutical development. While these technologies may accelerate vaccine production and disease research, experts warn that they could also simplify the manipulation or enhancement of dangerous biological agents.

8.6 South Korea – AI Surveillance during the COVID-19 Pandemic

South Korea, Artificial Intelligence Surveillance During the COVID-19 Pandemic

In 2020, during the coronavirus pandemic, South Korea established one of the best AI-based surveillance and contact tracing mechanisms to control the spread of the coronavirus. Following a massive infection linked to a church group called Shincheonji in the city of Daegu in early February 2020, the South Korean government fast-tracked its adoption of artificial intelligence and digital tools for detecting infections and identifying possible contacts.

Through mobile phones' GPS, CCTV cameras, credit card usage history, travel, transport, and health-related data, health professionals mapped out the movements of those infected. With the help of artificial intelligence technology, it was much easier and faster to analyze and handle such large volumes of data.

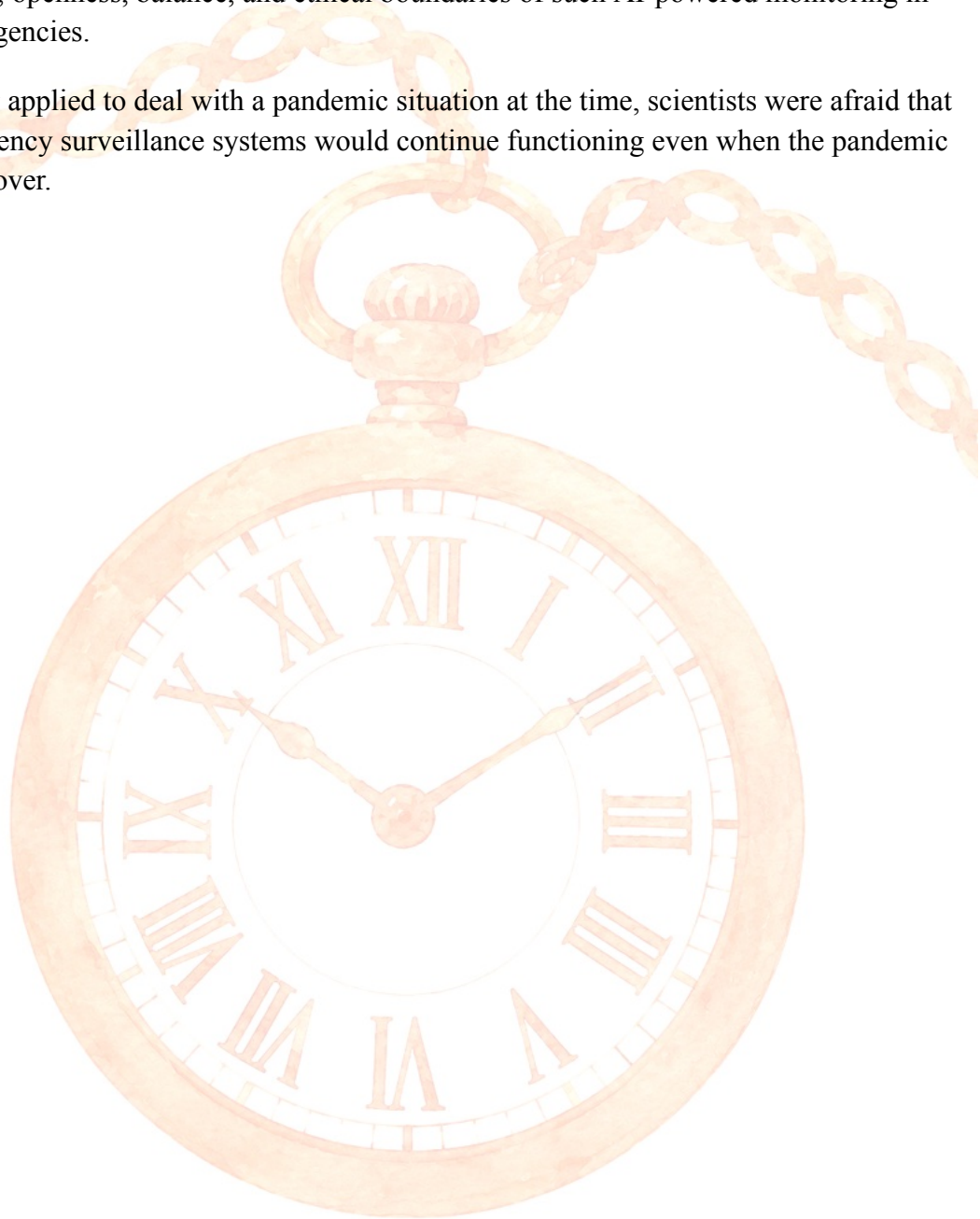
The reaction of South Korea gained significant attention in 2020 and 2021 due to its efficiency. The state managed to maintain relatively low levels of contagion in the early stages of the disease without imposing extensive lockdowns characteristic of other countries. In fact, the implementation of AI surveillance demonstrated the potential that digitalization had for addressing public health issues in the context of global pandemics.

On the other hand, such a solution to the problem generated considerable ethical and social controversies linked to the violation of people's privacy rights and intrusive governmental surveillance. The collection of too much personal data resulted in mass monitoring and abuse of surveillance tools, which eventually led to privacy breaches and public protests. For example, in 2020, detailed data about the routes taken by infected people was revealed

publicly, causing privacy invasion and stigma being made public, resulting in breaches of privacy, stigma, and attacks from civil rights organizations.

This South Korean story emerged as one of the main examples demonstrating the conflict between public health security and individual rights in the new digital world. Although the innovations helped address the problem efficiently, many key questions arose around issues like consent, openness, balance, and ethical boundaries of such AI-powered monitoring in health emergencies.

While being applied to deal with a pandemic situation at the time, scientists were afraid that these emergency surveillance systems would continue functioning even when the pandemic was finally over.



9. Questions a Resolution Must Answer

1. How can international humanitarian law and the Biological Weapons Convention be adapted to address emerging threats posed by AI-enabled synthetic biology and automated pathogen engineering?
- 2.
3. How can the international community balance rapid scientific collaboration during pandemics with the need to restrict access to sensitive biological data that could be exploited for hostile purposes?
4. How can healthcare systems identify and eliminate epistemic risk caused by excessive dependence on AI-generated medical predictions and diagnostic recommendations?
5. How can governments prevent emergency AI surveillance systems introduced during pandemics from evolving into permanent mechanisms of mass surveillance and social control?
6. What mechanisms can prevent AI-generated misinformation, false outbreak predictions, or manipulated health data from causing mass panic, discrimination, or political destabilization during pandemics?
7. To what extent should private biotechnology corporations and AI developers be held legally liable for biosafety failures, harmful medical predictions, or unethical applications of their technologies?
8. To what extent should AI-assisted biological research be classified as dual-use technology under international biosecurity law, and how can regulation prevent weaponization without suppressing legitimate scientific advancement?
9. What safeguards are necessary to prevent cyberattacks, unauthorized access, or geopolitical misuse of AI-integrated biological research facilities and genomic databases?
10. How can countries regulate open-source AI models and publicly accessible genomic databases that may unintentionally enable the creation or enhancement of dangerous pathogens?
11. What safeguards are needed to tackle the ethical and legal challenges that arise when AI systems are used to prioritize patients, allocate scarce medical resources, or influence end-of-life healthcare decisions during public health crises?

10. Conclusion

Advancements in AI and its integration into the field of medicine have rapidly transformed how medical research and diagnosis are conducted. It has transformed how diseases are detected and diagnosed in the wake of a pandemic through faster data analysis, predictive modelling, genomic sequencing, disease surveillance systems, and accelerated vaccine and treatment development. Additionally, advancements in biotechnology and GoF research have enabled scientists to better understand pathogens, strengthen disease prevention strategies, and improve medical research.

Although AI aids in the early detection of diseases, accelerated research, and speeds up treatment, there are various ethical issues surrounding this. Biosecurity risks, algorithmic bias, misdiagnosis, epistemic risk, and unequal access to technology are a few of these. One of the main concerns is algorithmic bias, where AI models may produce flawed results due to incomplete or inaccurate training data. Technologies that are intended for medical advancement can also be misused in harmful ways, particularly in the context of dual-use biotechnology and AI-assisted biological research. The increasing integration of AI into gain-of-function research and pathogen analysis has further raised concerns regarding biosafety, laboratory security, and the potential misuse of biological research.

If a disease is misdiagnosed, then it can erode doctor–patient relationships and affect patient mental health and well-being. Stakeholders play a key role in overseeing medical AI models. Governments are responsible for overseeing the implementation of such models, AI developers are responsible for creating safe and transparent AI models, civil society is responsible for spreading awareness in case of a public health crisis, and the media plays an important role in communicating information between the government and the public.

The committee should address these concerns and protect human rights while keeping in mind the UNESCO Universal Declaration on Bioethics and Human Rights, along with international collaborations.

11. Guide to Research and Sources

The purpose of this guide is to give delegates an in-depth understanding of the agenda, with topics discussed ranging from biosecurity threats in AI and biases in the algorithms to stakeholders involved and the many ethical, legal and technological implications associated with them. Nevertheless, this guide should serve merely as a beginning point. Each delegate must go out into their own research and come to the committee with in-depth knowledge of the agenda as a result.

Since this particular agenda is both highly technical and constantly evolving, the quality and reliability of sources is vital. Data concerning AI technology and biosecurity practices are changing fast, and incorrect or outdated information will significantly hinder discussion. While mainstream news outlets are a great resource in providing information regarding background, we advise delegates to refer to internationally recognized organizations for all statistical claims, scientific theories and policies. Since this agenda is quite delicate in the sense of bioethics and biosecurity, it is very important for delegates to make sure that information comes from credible sources in the committee.

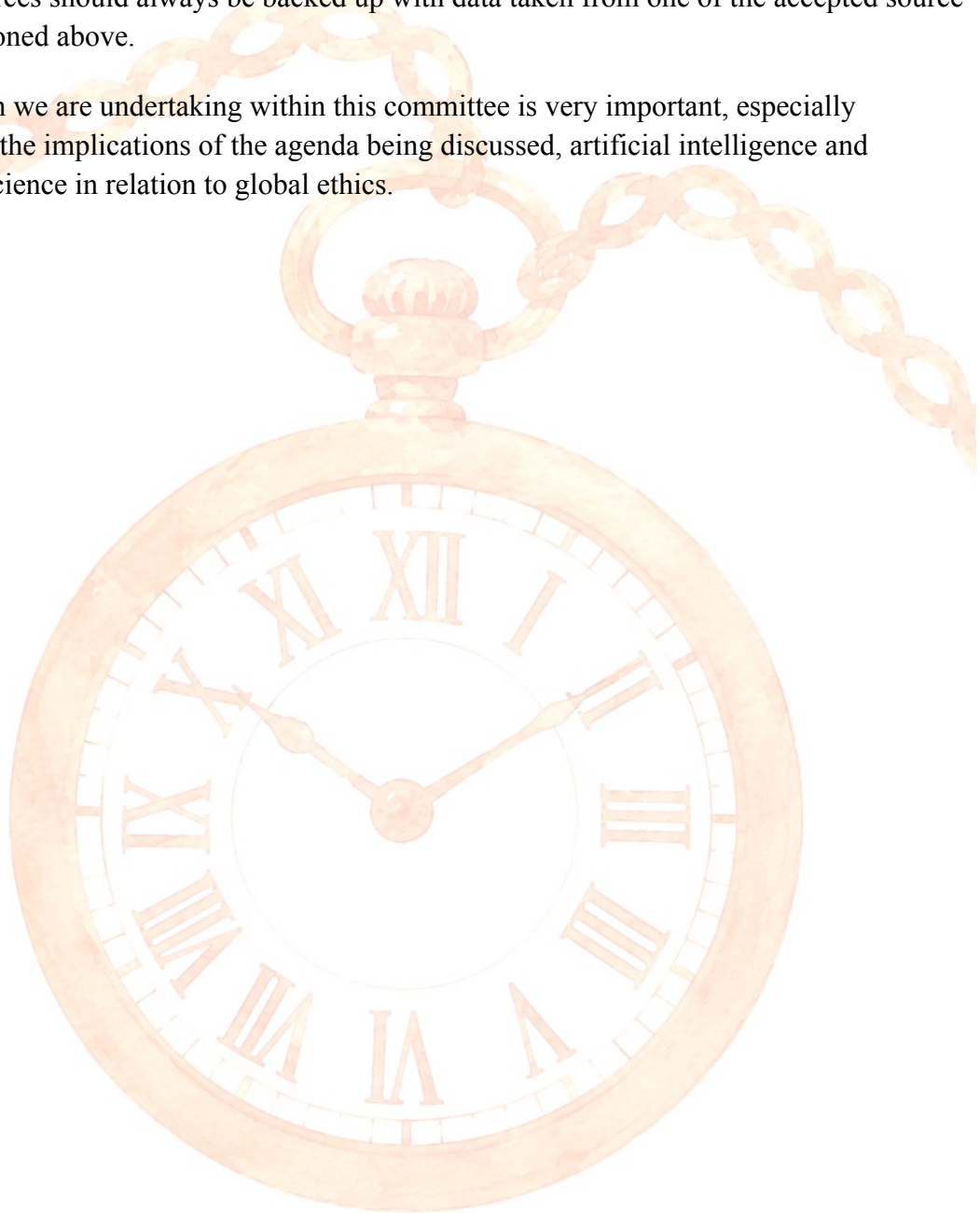
It is also advisable that participants verify important figures and data provided in various reports where applicable. The strength of the figure provided in one report will certainly be fortified by another independent source, which provides an additional piece of information on the same issue. This is critical for emerging facts on issues of AI performance, diseases, and international regulation.

The sources used by this committee are of the following kinds:

- 1) Peer-reviewed academic journals and published scientific literature (including PubMed, PubMed Central, and journals such as PLOS Digital Health, Applied Biosafety, and Nature)
- 2) Reports and publications from United Nations bodies and UN-affiliated organisations, including the WHO, UNEP, UNESCO and the UN Office for Disarmament Affairs
- 3) Reports from intergovernmental and strategic organisations such as the OECD, the World Bank, the European Union, the African Union and ASEAN
- 4) Publications from established policy research institutions and think tanks such as RAND Corporation, the Johns Hopkins Center for Health Security, and the Center for AI Safety (CAIS)
- 5) Official government statements, legislative documents, press releases and national public health agency reports (such as those from the CDC or NIH)
- 6) Humanitarian organisations and global health bodies with a demonstrated track record of independent, evidence-based reporting
- 7) Internationally recognised news organisations such as Reuters, Associated Press and Al-Jazeera, for factual and contextual reporting

Delegates should also keep in mind that although some sources can be good to develop basic knowledge about an issue, they cannot be used on their own as a foundation for making statements in committees. Examples include information taken from Wikipedia, social media pages, personal blogs, and reports that have not been peer-reviewed or come from institutions with no apparent institutional accountability. While sources like these might provide a starting point for research or help in identifying leads for research, any information provided by such sources should always be backed up with data taken from one of the accepted source types mentioned above.

The research we are undertaking within this committee is very important, especially considering the implications of the agenda being discussed, artificial intelligence and biological science in relation to global ethics.



12. Bibliography

1. [World Health Organization – Health Systems](#)
2. [World Health Organization – Disease Outbreaks](#)
3. [World Health Organization – Ethics and Governance of Artificial Intelligence for Health](#)
4. [Centers for Disease Control and Prevention – Surveillance Resource Center](#)
5. [National Institutes of Health](#)
6. [Johns Hopkins Center for Health Security](#)
7. [World Bank – Health](#)
8. [OECD AI Principles](#)
9. [World Economic Forum – How AI Can Transform Patient Care and Treatment](#)
10. [World Economic Forum – Scaling Smart Solutions with AI in Health](#)
11. [U.S. Department of State – Biosecurity and Civil Society](#)
12. [ScienceDirect – Public Participation and Health Risks](#)
13. [Australian Government – Media Guidelines During Outbreaks](#)
14. [PubMed Central – Challenges of AI in Healthcare](#)
15. [PubMed Central – Limitations of AI in Disease Detection](#)
16. [Bioethics in the 21st Century: Challenges and Perspectives](#)
17. [RAND – AI and Biosecurity Report](#)
18. [SAGE Journals – Stakeholders in Biosecurity](#)