Letter To Member States Of The World Health Organization

10 February 2026

Biosecurity Issues In The PABS Negotiations

We, the undersigned organizations, and academics, write to express our serious concerns over the insufficient attention being given to biosecurity risks and preventive safeguards in the ongoing negotiations on the Pathogen Access and Benefit Sharing (PABS) Annex to the WHO Pandemic Agreement.

Rapid advancement of artificial intelligence and synthetic biology is outpacing existing biosecurity frameworks, (such as using a list of "sequences of concern" for screening orders for synthetic DNA), while cheaper and accessible sequencing/synthesis benchtop devices shift risks upstream to pathogen identification, sequence data access, and bioinformatic analysis.

General references in the draft PABS text to existing international and national laws on biosafety, biosecurity, export controls and data protection are insufficient for a global system facilitating access to dangerous pathogens and their genetic blueprints. International law offers limited tools to monitor and regulate dual-use research, despite pandemic-capable pathogens often being studied in biodefense programs. Relying on individual States for the biosecurity of PABS infrastructure means relying on fragmented, uneven safeguards that weakens global biosecurity and enables arbitrary or politically motivated restrictions on legitimate science.

More fundamentally, the recent Bureau proposed PABS draft text does not adequately address the new biosecurity risks created by the system itself especially in the context of rapid rise of AI. The Bureau's draft text does not explicitly require recipients of pathogen samples and sequence data to be identified and bound by contractually enforceable obligations. Effective traceability measures are also missing.

Once pathogen sequences are made widely available, physical transfer of samples is no longer necessary to create new dangerous agents. Using openly available reverse genetics protocols, synthetic DNA corresponding to a pathogen genome can be assembled with minimal oversight.[1] At present, there are few requirements for users of sequence data to report the creation of synthetic sequences and/or materials derived from shared information. Cybersecurity threats further compound these risks: sequencing machines, databases, and analytical tools can be targeted or manipulated, and AI systems are already capable of generating novel sequences that bypass existing screening frameworks.[2]

Even a low-probability event - such as a laboratory accident or diversion could have consequences exceeding those of the COVID-19 pandemic. Anonymous or unconditional access to pathogen sequence data significantly increases the risk of misuse, whether accidental or deliberate. The possibility of coordinated malicious use, including the assembly
and release of multiple pathogens using anonymously accessed sequences, is much more than a purely theoretical threat.[3]

Opposition to user registration when accessing pathogen databases is therefore deeply concerning. Such opposition as usually argued is not justified by open-science principles, since UNESCO's Open Science Recommendation (2021) requires governments to prevent or mitigate harmful effects of scientific applications and be vigilant about such consequences of open science infrastructure.

A paper[4] assessing potential cybersecurity weakness in pathogen genome databases has found that: *"Many databases reviewed in this article contain components that do not require login. Users can simply use a web interface to query data from databases such as NCBI, EMBL-EBI, and many other specialized databases. Users also can use a programming language, a REST API, or a MySQL query to access data. For batch download, anonymous FTP access is provided in several cases.... No databases reviewed in this article require two-factor authentication or login through third party accounts. Requiring strong passwords, implementing two-factor authentication, and implementing login through third party accounts (Google, ORCID, or institution-specific accounts) could provide additional security measures for the current generation of genomic databases."*

These risks are amplified by the global expansion of high-containment laboratories,

mobile laboratories, databases, biofoundries, and the emergence of cloud laboratories, where experiments can be conducted remotely. Such facilities may become targets for cyberattacks or sites of misuse if not properly governed. A EU funded study also highlights that malicious actors could also remotely manipulate synthetic DNA orders to encode harmful agents.[5]

Notably, WHO's 2024 Laboratory Biosecurity Guidance[6] also refers to applying a standard material transfer agreement while transferring high-consequence material, and to include policy about the publication of information (data) generated using such materials, along with other rights and obligations of the provider and the recipient of the material and any other person involved in such agreement. An earlier WHO document clearly recognizes that genetic information can be used maliciously.[7] EU Regulation on Health Data Spaces also prohibits certain types of secondary use of data and calls for robust governance and transparent models of user access in databases.[8]

While we appreciate the objective of the PABS system, rapid sharing of pathogens with pandemic potential and the rapid sharing of benefits on an equal footing, it would be highly irresponsible of WHO and its Members to downplay and underestimate the biosecurity implications of such a system. Resistance to robust security mechanisms, especially traceability, does not reflect contemporary realities in biotechnology and digital science and the rise of artificial intelligence.

We, therefore, recommend that the PABS Annex:

1. Require all recipients of pathogen samples and/or sequence information to be clearly identified and bound by legal contractually enforceable minimum biosafety and biosecurity obligations. Verified user identities and enhanced transparency has become very critical for biorisk management.[9]
2. Mandate reporting to WHO of research activities that alter pathogen characteristics in ways that increase pathogenicity or pandemic potential.
3. Ensure that laboratories and databases serving as repositories are accountable to WHO Member States and maintain transparent logs of access and use.
4. Obligate users to report laboratory accidents, laboratory-acquired infections, and any compromise of digital infrastructure.
5. Establish robust track-and-trace mechanisms, potentially using advanced digital technologies, to ensure transparency and accountability.

We submit these concerns and recommendations in the interest of strengthening the PABS system so that it advances equity and global public health, without being the source of new and avoidable risks.

Signed,

Signatures are in a personal and institutional capacity.

Scientists And Scientific Organizations

European Network of Scientists for Social and Environmental Responsibility (ENSSER) Europe

Federation of German Scientists Germany

Institute for Independent Impact Assessment of Biotechnology (Testbiotech) Germany

National Platform on Radiation Risk (NPS) Europe

Union of Scientists Committed to Society and Nature of Latin America (UCCSNAL) Latin America

Angelika Hilbeck Retired professor at the Federal Institute of Technology Zurich (ETH)

Dieter Hammer Emeritus Professor at the Eindhoven University of Technology and University of Groninger (Netherlands)

Jack A Heinemann Professor at the University of Canterbury and Director of the Centre for Integrated Research in Biosafety (New Zealand)

José Luis Yela Professor at the University of Castilla-La Mancha (Spain)

Civil Society Organizations

Action Group on Erosion, Technology and Concentration (ETC Group) Global

African Centre for Biodiversity Africa

Biodiversity and Biosafety Association of Kenya (BIBA) Kenya

Ecological Action Ecuador

EcoNexus Global

Friends of the Earth United States

Global Health Responsibility (GHRA) Austria

International Association for Indigenous Peoples' and Community Conserved Areas and Territories (ICCA Consortium) Global

IT for Change India

Navdanya International Global

POLLINIS France

Society for International Development Global

Southeast Asia Regional Initiatives for Community Empowerment (SEARICE) Southeast Asia

Terre A Vie Burkina Faso

Third World Network Global

Notes & References

[1] Hearing before The Subcommittee on Emerging Threats and Spending Oversight of The Committee on Homeland Security and Governmental Affairs, United States Senate, One Hundred Seventeenth Congress, Second Session, August 3, 2022; Combined Study On Digital Sequence Information in Public and Private Databases and Traceability, Convention on Biological Diversity, AHTEG 2020.

[2] Nasreen Anjum et. al (2025), Cyber-Biosecurity Challenges in Next-Generation Sequencing: A Comprehensive Analysis of Emerging Threat Vectors. IEEE Access, 13. pp. 52006-52035; Boris A. Vinatzer et. al (2019), Cyberbiosecurity Challenges of Pathogen Genome Databases, Front. Bioeng. Biotechnol., 15 May 2019

[3] Robert F. Service (2023), Could chatbots help devise the next pandemic virus?, *Science*, reports a classroom experiment with graduate students demonstrating AI could help someone with no science background and evil intentions order a virus capable of unleashing a pandemic. See also, Credible pandemic virus identification will trigger the immediate proliferation of agents as lethal as nuclear devices, T*estimony before Senate Homeland Security and Governmental Affairs Committee, Subcommittee on Emerging Threats and Spending Oversight* in Aug 2022.

[4] Boris A. Vinatzer et. al (2019), Cyberbiosecurity Challenges of Pathogen Genome Databases, Front. Bioeng. Biotechnol., 15 May 2019

[5] A European Union funded study by the United Nations Institute for Disarmament Research (UNIDIR)'s Weapons of Mass Destruction Programme (WMD) and Security and Technology Programme (SECTEC) notes that
"The number of facilities across the world handling dangerous pathogens and toxins is increasing alongside the growth of the bioeconomy. In addition to an estimated 51 existing Biosafety level (4) (BSL-4) laboratories,18 more are reportedly underway or planned across the globe.19 BSL-2 and BSL-3 laboratories that are capable of undertaking research on dangerous pathogens, are also understood to be increasing in number." The UNIDIR study further says, *"malicious cyber actors could also interfere with the physical components of a biological research and development facility, such as the supervisory control and data acquisition systems. Such interference could hamper the capabilities of the laboratory to deliver immunization compounds in times of a pandemic or could disable mechanisms preventing the accidental release of deadly pathogens. Research has also illustrated that malicious actors could remotely interfere with synthetic DNA orders to encode harmful agents".*

[6] WHO, *Laboratory biosecurity guidance*, 21 June 2024.

[7] WHO, *Global guidance framework for the responsible use of the life sciences*, 2022, states: *"The increasing development of large health data sets, research and DNA databases, the digitization of health data and the increasing use of integrated data require biodata to be well managed to ensure that these data are not exploited to cause harm. Biodata for research and development have dual use potential. Access to data is critical during health emergencies and for health research. At the same time, the risk that data might be misused for harmful purposes requires mechanisms and expertise that ensure these data are kept secure. Safe and secure data management (e.g. through the use of cyberbiosecurity) is an integral part of biorisk management."*

[8] Articles 54 and 60 respectively of the Regulation (EU) 2025/327 of The European Parliament and of The Council of 11 February 2025 on The European Health Data Space.

[9] United Nations Institute for Disarmament Research, Cyberbiosecurity: Emerging risks and opportunities for the Biological Weapons Convention, Technical Brief, Thursday, 4 December 2025; David Stiefel et. al, Enhancing Transparency for Bioscience Research and Development, Nuclear Threat Initiative, BIO. August 2025.