Version: 10 February 2016

Global Alliance for Genomics and Health: Accountability Policy

Preamble

The Global Alliance for Genomics and Health ('GA4GH') is an international, non-profit coalition of individuals and organizations working in healthcare, research, disease advocacy, life science, and information technology dedicated to improving human health by maximizing the potential of genomic medicine through effective and responsible data sharing. Its mission is to accelerate progress in human health by helping to establish a common framework of harmonized approaches to enable effective and responsible sharing of genomic and clinical data.

Openness and accountability between stakeholders are needed to foster trust and collaboration. This *Accountability Policy* is directed at stakeholders responsible for oversight of data sharing, and outlines best practices for monitoring and responding to non-compliance with data sharing standards (see definition, s. 2.3).[1] The Policy builds on the GA4GH *Framework for Responsible Sharing of Genomic and Health-Related Data* (the '*Framework*'), which sets forth a harmonized, human rights approach for responsible data sharing, based on four Foundational Principles:

- Respect Individuals, Families and Communities
- Advance Research and Scientific Knowledge
- Promote Health, Wellbeing and the Fair Distribution of Benefits
- Foster Trust, Integrity and Reciprocity

The *Framework* identifies 'Accountability' as a core element for responsible data sharing, and encourages stakeholders to:

- Put in place systems for data sharing that respect the Framework,
- Track the chain of data access and/or exchange to its source,
- Develop processes to identify and manage conflicts of interest, and
- Implement mechanisms for handling complaints related to data misuse; for identifying, reporting and managing breaches; and for instituting appropriate sanctions.

Other data sharing best practices can be found in the specific policies of the GA4GH, including the Consent Policy and Privacy and Security Policy. Links to additional sources of procedural guidance relating to accountability can be found in Appendix 3.

[1] As the GA4GH is not itself an oversight body, this policy does not address the accountability of members to the GA4GH.

I. Context

1. Context. The significant public health imperatives for the translation of new genomics knowledge, coupled with rapid technological developments, scientific advancements in genomics, and the increasingly global scale of data sharing, reinforce the need for a framework to ensure accountability, and in turn trust, between stakeholders. Individuals asked to share their data for broad research purposes, together with the ethics bodies responsible for protecting their interests, are asked to trust in a diverse, distributed cast of stakeholders around the world. Data sharing standards continue to emerge from a variety of sources, including consent processes, laws, regulations, and policies established by funding agencies, journals, institutions, large research projects and research consortia. Data stewards impose additional conditions on data use through access agreements. Even in contexts where data sharing standards are clearly established, however, policies and processes for monitoring and responding to non-compliance may be lacking. The community largely relies on employers or guarantors of data users to hold them accountable, but these institutions may lack the necessary resources, incentives, or expertise to do so effectively. Transparency in this and other contexts is crucial for accountability. If data stewards are not open about data availability and access processes, it is difficult to assess if data is fairly and effectively available. If data users do not take steps to demonstrate that use limitations are respected, it is difficult to assess if they are accountable for the data entrusted to them. To ensure accountability between stakeholders and respect for the *Framework*, there is a need for clear data sharing standards, openness about data handling practices, as well as policies and processes for monitoring and responding to non-compliance with local standards.

2. Interpretation.

2.1 For the purposes of this Policy, ‘data sharing’ includes, but is not limited to, the use, viewing, transfer, linkage, or exchange of data between the data donor and another party, or between a data steward and a third party, either openly or under specified access conditions. Data sharing may occur without having the data move from one place to another.

2.2 Stakeholders include, but are not limited to, researchers, bioinformaticians, IT experts, research participants and patient communities, journal publishers, research funding agencies, data protection authorities, academic institutions, hospitals, clinicians, research ethics committees, the life sciences and pharmaceutical industry, governments and government agencies, and public health organizations.

2.3 This policy addresses compliance with ‘data sharing standards’, by which it means *locally applicable* data sharing standards derived from laws, regulations, guidelines, policies and agreements. This policy only applies to GA4GH best practices to the extent they are adopted locally.

3. Definitions. A number of terms used in this Policy are defined in the GA4GH Data Sharing Lexicon.

4. Application. This policy is addressed to individual and organizational members of the GA4GH, as well as the broader community of stakeholders involved in data sharing. Section II outlines best practices for monitoring and responding to non-compliance with data sharing standards, and is primarily directed to stakeholders involved in the oversight of data sharing and data users (in research, the clinical sector, or industry). Section III outlines best practices for transparent and accountable data sharing, addressed to specific stakeholder groups.

II. Best Practices: Monitoring and Responding to Non-Compliance

Stakeholders involved in oversight of data sharing and data users (e.g., employers or guarantors) should establish clear policies and processes to address cases of non-compliance. In the context of this Policy, non-compliance should be understood in relation to locally adopted data sharing standards. Categories of non-compliance may include:

- Data misuse (non-compliance with applicable laws, regulations, guidelines, policies, approved protocol, or access agreements);
- Data breach (the wrongful release of data, whether as a result of accident, negligence or malice);
- Data hoarding (unreasonable or unjustified withholding of data);
- Non-compliance with security procedures;
- Provision of inaccurate or incomplete data or information (e.g., in data submission, access application, or progress report);
- Failure to obtain prior ethics approval before starting a research project, if required;
- Failure to appropriately acknowledge the efforts of contributors;
- Failure to respect benefit sharing requirements; or
- Inadequate supervision of research by an employer or guarantor.

Such policies and processes should aim to mitigate harm, deter future non-compliance, and educate stakeholders to prevent future non-compliance, in order to maintain trust in the research enterprise. The system established to monitor, adjudicate, and respond to non-compliance should be proportionate to the risk and harms of non-compliance. Responses to non-compliance may be either facilitative or punitive. It may be premature to apply punitive sanctions where data sharing standards are still evolving, and they cannot be applied at all in the absence formal oversight. To enhance accountability throughout the research ecosystem, stakeholders must collaborate to establish common data sharing standards; shared definitions of non-compliance; common monitoring, reporting, and investigation processes; as well as consistent responses to non-compliance.

Monitoring

Stakeholders involved in the oversight of data sharing and data users should respond in a timely and consistent manner to reports of non-compliance. Where feasible, an officer should be designated to handle and investigate such complaints. The name, role, and contact information of this officer should be made publicly available. Fair and transparent processes for investigating complaints of non-compliance should be established. It should be made clear in advance 1) that the parties are to be constructively involved in investigations, and 2) what consequences will apply if a party fails to provide assistance. All communications during an investigation should be logged, and kept confidential throughout to protect those under investigation from reputational harm.

Responding to Non-Compliance

A range of appropriate responses or sanctions (minimum to maximum) should be defined and made available for each category of non-compliance. Depending on the seriousness of the non-compliance and the type of stakeholder(s) involved, responses may include:

- Call for an explanation;
- Additional training;
- Financial or technical aid;
- Warning;
- Compliance audits;
- Suspension/termination of employment;
- Suspension/termination of access;
- Suspension/termination of related services;
- Suspension/termination of funding;
- Suspension/retraction of publication; or
- Report of non-compliance to:
    - Data steward(s) who provided the data;
    - Data donor(s) who provided the data;
    - The employer of the data user;
    - The ethics body responsible for the project;
    - Funders, data stewards, or journals implicated in the research;
    - Regulatory authorities or law enforcement officials; and/or
    - The general public.

Criteria should be defined for assessing the severity of a sanction, for example, first or repeat non-compliance; non-compliance not self-reported in a timely manner; sensitivity of data; or impact on data donors, data stewards, or vulnerable populations. Where repeated incidents occur at the same institution, it may be appropriate to apply sanctions both to individual researchers

and to the institution. In assessing non-compliance, elements of procedural fairness should be respected, including transparent, fair, and independent adjudication, a reasonable opportunity for affected parties to be heard, and specification of circumstances where an appeal is possible (e.g., when substantial sanctions are applied).

To improve collective knowledge of non compliance events, the compliance officer (or other person) should prepare a summary log of the nature of each non-compliance event and how it was resolved. This information should only be released once the non-compliance has been resolved, and should not identify the parties involved. Such a log would provide important data on the frequency, nature, and source of non-compliance events for future policy development.

III. Best Practices: Stakeholder-Specific

This section outlines stakeholder-specific best practices for enhancing transparency of data sharing practices. Additional accountability elements found in the GA4GH Consent Policy and Privacy and Security Policy are listed in Appendix 2. It does not represent an exhaustive list of stakeholders or practices.

Data Stewards

- Design consent and access processes that remove unnecessary use restrictions on data.
- Provide clear information about how data can be accessed and how requests are reviewed.
- Justify any use restrictions or refusals to provide access.
- Adopt standard or (preferably) common access processes between data sources where appropriate.
- Permanently link data with metadata about provenance and associated obligations and restrictions in a standard and machine-readable format.
- Maintain an auditable record of all data users and purposes for which access is provided, and where feasible make it available to data donors and the general public.
- Where feasible, delegate access decisions to an independent, external party.
- Clearly set out the consequences of a failure to respect access conditions.

Data Users

- Take reasonable steps to become familiar with use conditions, to establish whether an intended use is appropriate (e.g., by contacting the author or data steward), and to demonstrate that use conditions are respected.
- Identify and appropriately cite the sources of the data analysed.

Funders

- Recognize the importance of developing data resources in ranking proposals for funding.
- Provide adequate funding to support data sharing, as well as the effective monitoring, investigation, and enforcement of data sharing protocols.
- Gather information on the costs and effectiveness of compliance mechanisms to inform governance practices.

Journals

- Establish processes and timelines for making supporting datasets available that are integrated with article submission and ensure stable links between the publication and the dataset or a persistent and citable record of the dataset.
- Include a section in manuscripts or persistent links to information on how supporting datasets can be accessed, that describes and justifies any access restrictions.
- Take reasonable steps to require authors to demonstrate that secondary research is consistent with access conditions, and to appropriately acknowledge data sources.

Academic Institutions

- Educate trainees, current investigators, and ethics bodies (where applicable) on responsible data sharing practices through class work, mentorship, and professional development.
- Track data sharing contributions and give them due consideration when deciding hiring, tenure, and promotion decisions (where applicable).
- Provide infrastructure that facilitates the sending, receipt, and storage of data, including professional and technical capacity, and support for delivering data to repositories.
- Provide adequate resources for monitoring systems to encourage tracking of compliance, and establish clear processes for handling non-compliance by employees.

Ethics Review Bodies

- Members should be educated about the significance of and conditions for data sharing.
- Encourage researchers to plan to make their data available and to communicate this plan to data donors.
- Monitor respect of data sharing plans, and request a report demonstrating that protocols have been carried out.

Research Consortia

- Negotiate and reach clarity about roles and data sharing responsibilities before research begins.

IV. Implementation Mechanisms and Amendments

1. Attention should be paid to the interrelation of this Policy with other GA4GH guidance (e.g., Consent Policy, Privacy and Security Policy, Security Infrastructure).

2. Any stakeholder adhering to this Policy may propose one or more amendments to the present Policy by communicating the amendments to the GA4GH's Regulatory and Ethics Working Group (REWG). The REWG shall publicly circulate such amendments for comments and possible inclusion in this Policy.

3. The REWG, in collaboration with biomedical, patient advocacy, and ethical and policy organizations and committees, will track the adoption of this Policy and its application. It will also routinely review its provisions, be aware of advances in basic research and technology, and ethical and legal developments, and attempt to ensure that this Policy is fit for purpose.

V. Acknowledgements

This Policy is the result of the work of many people and committees. Developed under the auspices of the GA4GH's REWG, the Policy was formulated by an international committee, the Accountability Policy Task Team, which represented a wide spectrum of experts from the law, security, bioethics, genomics, life science industry, and clinical communities. Collaborative input was provided from individuals as well as biomedical, patient advocacy, and ethical, policy and legal organizations, committees, and projects from around the world (for contributors, see the Accountability Policy homepage).

Appendix 1

Policy Revision History

Policy Number/Version	Date Effective	Summary of Revisions

Appendix 2

Accountability Elements in Other GA4GH Specific Policies

Consent Policy

- The consent process, in any form it takes, should be properly documented.
- Consent materials and data sharing plans should be available for inspection and discussion with interested parties.
- Consent materials and data sharing plans should be updated and made available in response to new regulations and policies by responsible individuals within an organization or entity.
- Procedures should be in place to receive and respond to complaints or inquiries about policies and practices relating to consent to the sharing of genomic and health-related data. The procedures should be easily accessible and simple to use.

Privacy and Security Policy

- Data Stewards should clearly identify the individuals within their organization or entity who are responsible for data privacy, data management, and reporting procedures (including a contact person or contact point for complaints). Appropriate and regular training for the identified individuals to discharge these duties should be provided.
- Data Stewards should track new regulations, policies, expectations, and best practices, sharing these with responsible individuals within their organization or entity.
- Data Stewards and Data Users must comply with applicable privacy regulations and ethical norms at every stage of data sharing, and be in a position to provide assurances that privacy interests are appropriately protected when Data are collected, stored, processed, and shared.

Appendix 3

Suggested Procedural Guidance

- Administrative Data Research Network (ADRN), *Breaches Policy and Procedures* (2015) [link].
- Article 29 Data Protection Working Party (WP29), *Opinion 3/2010 on the Principle of Accountability* (2010) [link].
- The Canadian Institutes of Health Research (CIHR), the Natural Sciences and Engineering Research Council of Canada (NSERC), and the Social Sciences and Humanities Research Council of Canada (SSHRC), *Draft Tri-Agency Statement of Principles on Digital Data Management* (2015) [link].
- Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements a Document for Discussion* (2009) [link].
- Council of Canadian Academies (The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation), *Accessing Health and Health-Related Data in Canada* (2015) [link].
- The Future of Research Communications and e-Scholarship (FORCE11), *Guiding Principles for Findable, Accessible, Interoperable and Re-Usable Data* (2014) v B1.0 [link].
- Hrynaszkiewicz I et al, *Preparing Raw Clinical Data for Publication: Guidance for Journal Editors, Authors, and Peer Reviewers* (2010) *BMJ* [link].
- Hrynaszkiewicz I et al, *Publishing Descriptions Of Non-Public Clinical Datasets: Guidance For Researchers, Repositories, Editors And Funding Organisations* (2015) [link].
- Mascalzoni D et al, *International Charter of Principles for Sharing Bio-specimens and Data, European Journal of Human Genetics* (2014) *EJHG* [link].
- National Institutes of Health, *NIH Guide: Final NIH Statement On Sharing Research Data NOT-OD-03-032* (2003) [link].
- Nuffield Council on Bioethics, *The Collection, Linking And Use Of Data In Biomedical Research And Health Care: Ethical Issues* (2015) [link].
- Piwowar HA et al, *Towards a Data Sharing Culture: Recommendations for Leadership from Academic Health Centers* (2008) *PLoS Medicine* [link].
- Toronto 2009 Data Release Workshop Authors, *Benefits and Best Practices of Rapid Pre-Publication Data Release* (2009) [link].
- Wellcome Trust Expert Advisory Group On Data Access (EAGDA), *Establishing Incentives And Changing Cultures To Support Data Access* (2014) [link].
- Wellcome Trust Expert Advisory Group On Data Access (EAGDA), *Governance of Data Access* (2015) [link].
- Wellcome Trust Expert Advisory Group On Data Access (EAGDA), *Statement for EAGDA Funders on Re-Identification* (2013) [link].
- Wellcome Trust, Medical Research Council, UKCRC, and Cancer Research UK, *Good Practice Principles for Sharing Individual Participant Data from Publicly Funded Clinical Trials* (2015) [link].
- United Nations Environment Programme (UNEP), *Issues of Compliance: Considerations for the International Regime on Access and Benefit Sharing* (2010) [link].