ACTaccelerator
ACCESS TO COVID-19 TOOLS

FRAMEWORK FOR THE GOVERNANCE OF PERSONAL DATA FOR THE

Access to COVID-19 Tools Accelerator

1. CONTEXT

The Access to COVID-19 Tools (ACT) Accelerator was launched in April 2020 and brings together governments, scientists, businesses, civil society, philanthropists and global health organizations. Its purpose is to end the COVID-19 pandemic by scaling up the development and equitable distribution of tests, treatments and vaccines to all.

To achieve this purpose, there is a need to rapidly scale up research and development (R&D) into new products and digital tools. An effective response to COVID-19 requires access to, and use, linking and sharing of, personal data, and by extension, a critical requirement is the timely access to personal data that may be collected and stored by laboratories, hospitals, clinics, biobanks, medical devices and other digital tools. The use of these data raises many concerns including individual and group privacy, risks of stigmatization of and discrimination against individuals, groups and minority populations, in addition to other risks that arise depending on the context in which the data are used and the vulnerabilities of the individual or population. While these potential harms can manifest globally, there is no common standard. As much of these personal data are sensitive health data, many states have restricted or tightly controlled their use under national and regional data protection and privacy regulations and frameworks. However, many jurisdictions either do not have any equivalent data protection frameworks, or they may be lacking, resulting in uncertainty as to the acceptable uses of the data. While issues arising as a consequence of discrepancies between data protection frameworks are not uncommon, **it is critical in the current context of pandemic that there is a shared framework to enable the use of data for the ACT-Accelerator.**

IT IS ESSENTIAL THAT THE USE OF PERSONAL DATA IN RESPONDING TO COVID-19 APPROPRIATELY PROTECTS THE FUNDAMENTAL RIGHT TO PRIVACY AND MITIGATES OTHER RISKS THAT CAN ARISE IN THE USE OF PERSONAL DATA.

The ACT-Accelerator recognizes that the right to privacy is not absolute and can be derogated from on grounds of public health. This can only be done when necessary and proportionate, and where there are appropriate safeguards in place with consequences for failing to uphold these safeguards. The ACT-Accelerator recognizes that while the right to privacy may be limited in responding to COVID-19, there is a clear public interest in continuing to safeguard individuals' and communities' privacy, and to protect them to the extent possible from other risks associated with the use of personal data.

The use of personal data as part of a COVID-19 response must be done in a manner that is rooted in human rights which includes the right to privacy, the right to health and life, and the right to economic and social development. Continued access to personal data during COVID-19 is dependent on public trust, guarantees that only necessary information will be collected and accessed, and confidence in the use and protection of these personal data.

With this in mind, **this Framework provides a set of principles and procedural guidelines to guide the governance of personal data** so that privacy interests are respected while enabling the use of and access to such data to respond to COVID-19.

2. AIMS OF THE FRAMEWORK

This Framework adopts a principles-based approach embedded in a procedural guideline to the use of personal data to respond to COVID-19. It is intended to complement existing applicable national and international regulatory instruments on the use of personal data to enable access to and use of data without compromising fundamental rights.

This Framework aims to:

- **Promote best practice** and the responsible use of personal data in responding to COVID-19 in a manner that continues to safeguard privacy interests
- **Support the safeguarding of the rights of vulnerable groups** in a global context of inequality and asymmetries of power, taking into account that this vulnerability may arise due to co-morbidities, identity, personal circumstances, or the use of personal data without due consideration of possible harms
- **Complement national laws and policies** on data protection, surveillance, and the ethical conduct of research
- **Guide the development of national regulations** on the governance of data for COVID-19 related activities
- **Guide the development of mechanisms** for appropriate levels of community reviews and oversight
- **Be a dynamic framework** that responds to developments in the COVID-19 pandemic and engage with relevant stakeholders and communities to enhance this Framework.

3. GUIDING PRINCIPLES

This Framework is grounded on both substantive and procedural principles which should inform and guide initiatives funded by the ACT-Accelerator in the use and processing of personal data.

Substantive principles

Solidarity

The principle of solidarity acknowledges that we are interdependent and our individual well-being is dependent on the control and suppression of COVID-19 across the world. Solidarity must therefore underpin access to, the use and sharing of, data to advance knowledge that will be ultimately used to respond to COVID-19. The ACT-Accelerator aims to respond to a global need, and the use of data under this Framework must confer a clear public benefit on public health.

Respect for persons and communities

While the ACT-Accelerator is aware of the need for access to data, this may have implications for individuals, their families and their community. The collection and use of data must be done in a manner that respects individual persons and their wider community. The principle of respect for persons and communities is interconnected with the other principles of this Framework.

Respect for persons and communities requires the autonomy of the individual to be respected, but recognizes the interconnectedness of society and the importance of a societal response to COVID-19. It is thus important that key features of this response are communication, engagement and involvement with communities in decision-making on the use of data for COVID-19. In particular underrepresented and marginalized groups, including women and minorities in a given population, must be targeted.

Equity

The ACT-Accelerator is acutely aware of current global health disparities. Many marginalized groups and communities from resource-limited settings may not have access to healthcare, and this could have implications for access to COVID-19 tests, treatments and vaccines. The public health and economic impact of the pandemic will not be addressed unless there is equitable global access to COVID-19 tools.

Personal data are needed to develop COVID-19 tests, treatments and vaccines. The use of personal data should not perpetuate but ameliorate where possible global health inequity, exploitation and health disparities. Initiatives under the ACT-Accelerator are thus targeted at key vulnerable populations but with a global, lasting impact expected.

Non-exploitation

The use of data to respond to COVID-19 requires the involvement of individuals, communities and populations across the globe. This global effort must be respectful, collaborative and non-exploitative.

Data must be shared in line with national laws from where it originates, with the agreement of the data collector, and in line with the expectations of the individual and community.

It is essential that there are reciprocal benefits to the community and health system arising from the use of this data. These will undoubtedly be in the form of access to COVID-19 tests, treatments and vaccines, but benefits that include the capacity building and strengthening of health systems and other benefits identified through engagement should be discussed.

Privacy

Any limitation on the right to privacy in responding to COVID-19 must be necessary, proportionate, time-limited, and transparent. Accountability mechanisms must be put in place with provisions to safeguard the privacy of individuals and communities while personal data are processed for COVID-19 purposes. This is essential to help ensure that the digital tools developed to respond to COVID-19 are trustworthy. The use and disclosure of personal data in this context does not mean that privacy interests in data are extinguished.

Data stewardship

Data collected as part of a COVID-19 response are a valuable resource and initiatives under the ACT-Accelerator have a responsibility in enabling the sustainable and responsible use of these data.

The data must be accessible, accurate and adhere to best practices in data security and data management. An integral feature of data stewardship is that the use of the data is only to inform our understanding and to respond to COVID-19.

Procedural principles

Transparency

The collection, use of, and access to the data must be done in a clear and transparent manner. This requires transparent policies and procedures on the collection, protection, storage and use of the data throughout the data life-story.

Accountability

Transparent decision-making processes must be supported by accountable mechanisms to enable decision-makers to be held accountable. This can help promote trustworthiness.

Engagement

The use of data to respond to COVID-19 requires the involvement of many stakeholders. Decisions on collection, access, and use of these data should be made with the involvement of these stakeholders, including the data subjects. Such engagement must be genuine, involving the active and equal contribution of various stakeholders. It is particularly important that vulnerable groups, marginalized groups and groups at risk of discrimination are engaged with meaningfully.

4. IMPLEMENTATION OF GUIDING PRINCIPLES IN PRACTICE

The Framework applies to the processing of COVID-19 data in the execution of activities funded by the ACT-Accelerator. The ACT-Accelerator encourages individual countries and territories to adopt and follow the principles and guidelines as set forth in this Framework. This Framework applies to the collection, use, sharing and further processing of personal data in responding to COVID-19. The Framework applies to health surveillance, investigation, intervention, and research.

Biological samples will be collected, used and shared as part of a COVID-19 response. Many of the principles and procedures in this Framework apply equally. However, distinct issues arise in the governance of biological samples that are not necessarily present in personal data and as such require separate consideration.

Personal data	Any information that relates to an identified or identifiable individual.
Personal health data	Any personal data that relate to the health of an identified or identifiable individual.
Anonymized data	Any data that cannot identify an individual.
De-identification	Removing identifiers so an individual is not directly identified by the data. De-identified data fall under the scope of this Framework. De-identified data are not anonymous data. Re-identification is the process by which data are added to the de-identified data in order to make them identifiable.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, including collection, recording, access to, use, sharing, linking, storage, analysis, anonymization, or erasure, and in the context of this Framework refers to the use of personal data in responding to COVID-19 such as in R&D; evaluation of new diagnostic tools, therapies and vaccines; pandemic surveillance; and improvements to pandemic planning.

4.1 DATA COLLECTION AND STORAGE

Any limitation on the right to privacy must be necessary and proportionate to the aim of responding to COVID-19. This must continue only for as long as necessary to fulfil the processing aims or until WHO declares that COVID-19 is no longer a public health emergency of international concern (PHEIC), whichever comes first. The collection of personal data should be limited to the minimal amount of what is necessary to fulfil the objectives of responding to COVID-19.

Prior to the use of personal data, there must be consideration given as to whether the processing activity is likely to result in a high risk to the rights and freedoms of, or serious harm to, individuals or groups. If there is risk to rights and freedoms, or risk of serious harm, a risk assessment must be carried out prior to the processing of personal data.

This risk assessment must address:

- The risks to the rights and freedoms and other potential risks to the data subject and other groups
- How data subjects and the data derived from them will be protected and any relevant rights respected
- Third parties who may have access to the personal data and measures to mitigate unauthorized access
- Additional measures to be put in place to mitigate against the potential risks identified and monitor for unidentified risks.

4.2 DATA RETENTION

Retention of personal data must be time-bound. These personal data must be destroyed when the objective of the processing has been fulfilled or WHO declares COVID-19 to be no longer a PHEIC, whichever comes first. However, there may be justifiable reasons for retaining this personal data beyond this time limit. This may be due to a benefit to the individual (e.g. personal data are retained as part of the medical records of the individual) or a wider public benefit (e.g. data can enable a better understanding of pandemic response).

If personal data are to be retained beyond the period specified, the following must be met:

- There must be a benefit to the data subject or a public benefit. This benefit must be clearly identified and recorded
- Access to data must be restricted and subject to approval by a data access committee and an independent accredited ethics committee for research (if the personal data are to be used for research)
- Access to and use of these personal data must be in line with community expectations
- Benefit sharing arrangements must be discussed and agreed upon prior to access and use.

4.3 DATA MANAGEMENT

The ACT-Accelerator believes that an effective COVID-19 response is reliant on access to timely, secure and accurate data. All initiatives funded under the ACT-Accelerator have a responsibility for safeguarding the integrity of the data that they are processing. As part of this responsibility they must submit a data management plan (DMP). This DMP must make clear how the data will be kept secure and confirm that it will align with best practices in information security management (e.g. the ISO 27000 series and ISO/IEC 27002, GDPR). Initiatives funded under the ACT-Accelerator must allocate resources to align itself with these standards.

The DMP must describe measures to guard against unauthorized access to, disclosure, modification or destruction of the personal data. The DMP must commit to adhering to the FAIR (Findable, Accessible, Interoperable and Reusable) Principles.

As part of the DMP, it must be made clear whether the consent of the data subject has been or will be obtained. If consent will not be obtained, this should be noted in the DMP, as well as the justifications.

4.3.1 Processing with consent

Where individual consent can be obtained, **the data subject must be provided with clear, unambiguous language on the following:**

- The data to be collected and the purpose for which their personal data will be processed
- The duration of data storage
- The details of third parties likely to obtain access to the personal data
- Procedures for deciding on data access requests
- Measures and risk mitigation strategies and processes that are in place to safeguard the privacy of data subjects
- The process to be followed in the event of a data breach
- That they may withdraw their consent and the procedure to be followed so that they can easily withdraw
- Other rights they have in relation to the personal data.

THE CONSENT MUST BE VOLUNTARY AND THERE MUST BE NO DETRIMENTAL IMPACT TO AN INDIVIDUAL, INCLUSIVE OF ACCESS TO HEALTHCARE AND TREATMENT, IF THEY REFUSE TO GIVE CONSENT.

4.3.2 Processing without consent

Efforts must be made to obtain the consent of the data subject. However, the ACT-Accelerator recognizes that COVID-19 is a notifiable disease in many countries. The ACT-Accelerator also recognizes that due to the nature of the pandemic, it may not be practicable to obtain informed consent, and that data processing may be necessary for reasons of public interest in the area of public health. As such, the processing of personal data without consent is permitted provided it is exclusively for the purpose of responding to COVID-19, and that there are suitable specific measures in place to adequately safeguard the rights and freedoms of data subjects. As part of the DMP, the justifications for not obtaining consent must be noted.

Prior to the processing of personal data without consent for research, **all initiatives funded under the ACT-Accelerator must have approval from an independent accredited ethics committee for research.** In addition, the processing of personal data without consent must follow the applicable legal and ethical frameworks.

4.3.3 Secondary use of personal data

During the COVID-19 pandemic, the use of personal data for a purpose other than that for which they were collected may be required. This can maximize the value of the personal data in a COVID-19 response.

The secondary use of the personal data is permitted provided:

- Its use is in line with the applicable legal and ethical frameworks
- The secondary use has the approval of a data access committee
- The secondary use of personal data for research has been approved by an independent accredited ethics committee for research
- The views of the community have been sought through community engagement.

4.4 TRANSPARENCY OF DATA PROCESSES

Initiatives funded under the ACT-Accelerator have an obligation of transparency towards data subjects, the public, and the ACT-Accelerator when processing personal data.

In particular, the following must be made available in a clear and accessible manner:

- The objective and benefits of the processing
- The duration of data storage
- The details of third parties likely to obtain access to the personal data
- Procedures for deciding on data access requests
- Measures and risk mitigation strategies and processes that are in place to safeguard the privacy of data subjects
- The process to be followed in the event of a data breach.

4.5 RESPONSIBILITIES OF THOSE PROCESSING PERSONAL DATA

The processing of COVID-19 personal data must be done in a manner that respects and upholds the right to privacy of the data subjects. Any initiative funded under the ACT-Accelerator must identify in advance the individual(s) with the overall responsibility for compliance with this Framework.

THERE MUST BE GUARANTEES THAT THE INDIVIDUAL(S) HAVE SUFFICIENT RESOURCES TO FULFIL THEIR ROLE AND ENSURE COMPLIANCE WITH THIS FRAMEWORK.

In particular, this individual(s) is responsible for:

- Ensuring the privacy, integrity and security of the data
- Ensuring the safeguarding of the personal data in line with the principles of human rights and data protection
- Informing and educating anyone who will be processing personal data of their duties and responsibilities under this Framework as well as their legal obligations
- Regularly reviewing security procedures in place to ensure that they are compliant with the highest industry standards
- Putting mechanisms in place to guard against and respond to data misuse and data breaches
- Ensuring that any data breach is communicated to the data subject where possible, as well as to the public and the ACT-Accelerator, in a timely manner.

4.6 EQUITABLE ACCESS TO DATA

The ACT-Accelerator is aware that there is historically inequitable access to tests, treatments and vaccines. **Any initiatives funded under the ACT-Accelerator have a duty to ensure that there is equitable distribution of COVID-19 tests, treatments and vaccines.**

COVID-19 REQUIRES A GLOBAL RESPONSE. COLLABORATIONS BETWEEN DIFFERENT SECTORS OF SOCIETY AND INTERNATIONAL COLLABORATIONS ARE ESSENTIAL.

A key feature of these collaborations will be rapid access to and sharing of personal data. Any collaborations must be non-exploitative and ensure the equitable access to and sharing of personal data and equitable distribution of COVID-19 tests, treatments and vaccines. The ACT-Accelerator is aware that inequitable collaborations can be manifested in many ways.

With this in mind:

- The sharing of data must be done at no cost or at cost-recovery only
- Collaborations must consider community, individual researcher, and organizational benefits as part of benefit sharing and capacity development
- Local researchers must be involved in defining the research question
- The primary data collectors and anyone involved in knowledge production must be afforded appropriate recognition, for example, through co-authorship where appropriate
- Concrete steps must be identified to support local researchers in developing tools and resources to produce, access and analyse data
- Opportunities for developing scientific capacity (through infrastructure or personnel development) and/or governance capacity (through strengthening research ethics committees or data access committees) must be identified and agreed upon
- Access to COVID-19 tests, treatments and vaccines will be a clear benefit for local communities, but other benefit sharing arrangements must be discussed and agreed upon as part of community engagement.

4.7 PUBLIC ENGAGEMENT

A successful response to COVID-19 cannot occur without public support and involvement. The use of technology to develop tools as part of a COVID-19 response is valuable and necessary. The ACT-Accelerator is aware of the digital divide, and digital technologies must not further marginalize already disadvantaged and marginalized groups. Issues of local access, trust, privacy concerns, and other factors must be considered when developing tools under the ACT-Accelerator.

During the COVID-19 pandemic, large amounts of personal data are collected from entire populations that may include information on age, race, sex, health, ethnic group, and socio-economic factors. This information may be necessary to understand whether these factors contribute to differences in infection rates, as well as impact the effectiveness of tests, treatments and vaccines.

The ACT-Accelerator is aware that many marginalized groups have been and continue to be stigmatized and subject to discrimination. **It is essential that the processing of personal data does not result in stigmatization of or discrimination against individuals or groups or result in social harms to individuals or communities.**

EARLY PARTICIPATION AND ENGAGEMENT WITH DATA SUBJECTS, COMMUNITY REPRESENTATIVES AND CIVIL SOCIETY CAN HELP IDENTIFY POTENTIAL STIGMAS.

Any initiatives funded under the ACT-Accelerator must have a public engagement strategy that will:

- Establish a mechanism through which the public can give feedback on issues that include the processing activities and their implications, and any concerns relating to privacy
- Engage with people who have had or currently have COVID-19
- Describe how the public will be regularly updated on the outcomes of the processing of personal data, the benefits and advances made, as well as any set-backs
- Respect local cultural norms and describe and discuss the process of engagement with local leaders and community members.

5. DATA STEWARDSHIP OVERSIGHT COMMITTEE

The ACT-Accelerator recognizes the gravity of COVID-19 and the need for rapid access to and sharing of personal data, but equally recognizes the importance of robust data protection throughout this pandemic. It is incumbent upon governments to promote the responsible use of data during the COVID-19 pandemic. National data protection authorities (where in existence) have an important role to play. Governments themselves must be transparent and accountable in decisions taken as part of a COVID-19 response.

IT IS ALSO ESSENTIAL THAT THE PROCESSING OF PERSONAL DATA IS IN LINE WITH PUBLIC AND COMMUNITY EXPECTATIONS DURING THE COVID-19 PANDEMIC.

As part of this, the ACT-Accelerator strongly recommends the establishment of national independent Data Stewardship Oversight Committees for COVID-19. These interdisciplinary committees must include experts in public health, law (particularly privacy), ethics, technology, security, people who have or have had COVID-19, and representatives from marginalized groups, with a specific emphasis on those facing intersectional discrimination.

The immediate functions of the committee will be to:

- Monitor the collection, use and sharing of personal data during COVID-19 to ensure that the principles of this Framework are implemented, but also provide further guidance where necessary
- Commence a process of ongoing public participation throughout the pandemic on the use of personal data. This engagement must consider the wider ethical and social implications of the use of personal data that goes beyond data protection.

The medium- to longer-term functions of the committee will be to:

- Determine access to COVID-19-related personal data in line with the public interest once WHO declares COVID-19 to be no longer a PHEIC
- Develop evidence-based frameworks on the use of personal data for pandemics.

6. MONITORING AND EVALUATION OF THIS FRAMEWORK

This Framework is a living document and should be updated and refined based on recommendations and experiences with its implementation.

Feedback should be sent to the ACT-Accelerator Diagnostics Pillar (ACTAdiagnostics@finddx.org).

In addition, the R&D and Digital Working Group of the ACT-Accelerator Diagnostics Pillar must evaluate and update this Framework every 6 months.

ACKNOWLEDGMENTS

This Framework was commissioned and initiated by FIND as co-convener of the ACT-Accelerator Diagnostics Pillar. It was drafted by Ciara Staunton under the guidance of the R&D and Digital Working Group of the ACT-Accelerator Diagnostics Pillar. Carolyn Gomes, Michael Johnson and Ranga Sampath all provided substantial feedback through the R&D and Digital Working Group of the ACT-Accelerator Diagnostics Pillar.
Substantive feedback was provided by Susan Bull, Joshua Castellino, Ames Dhai, Edward Dove, Ehsan Shamsi Gooshki, Joelle Grogan, Oommen John, Stephanie Johnson, Deborah Mascalzoni, Natalie Mayet, Dianne Nicol, Mark Taylor, Dykki Settle, Oommen John on behalf of the COVID-19 Clinical Research Coalition Data Sharing Working Group, the ACT-Accelerator Ethics & Governance Working Group and the WHO Legal Department.

APPENDIX 1: RELEVANT DOCUMENTS

Joint Statement on Data Protection and Privacy in the COVID-19 Response (2020)

Council of Europe *Convention 108+ Convention for the Protection of Individuals with regard to the Processing of Personal Data*

Council of Europe *Convention on Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Convention)* (1997)

Council for International Organizations of Medical Sciences *International Ethical Guidelines for Health-related Research Involving Humans* (2016)

Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects

Declaration of Taipei: Research on Health Databases, Big Data and Biobanks

General Data Protection Regulation

Global Alliance for Health *Framework for responsible sharing of genomic and health-related data*

Global Research Collaboration for Infectious Disease Preparedness *Principles of Data Sharing in Public Health Emergencies (June 2018) Go FAIR FAIR principles* (2016)

H3Africa *Ethics and Governance Framework for Best Practice in Genomic Research and Biobanking in Africa*

Nuffield Council on Bioethics Research in global health emergencies: ethical issues (2020)

International Health Regulations 2005

OECD *Principles and Guidelines for Access to Research Data from Public Funding* (2007)

OECD *Recommendation of the OECD Council on Health Data Governance* (2017)

Office of the High Commissioner of Human Rights *A Human Rights-based Approach to Data* (2018)

UNESCO *Universal Declaration on Bioethics and Human Rights* (2005)

United Nations *Universal Declaration on Human Rights* (1948)

United Nations *Personal Data Protection and Privacy Principles* (2018)

World Health Organisation *WHO's Code of Conduct for Open and Timely Sharing of Pathogen Genetic Sequence Data During Outbreaks of Infectious Disease* (2019)