

Section A:
The Signal Code

Preamble

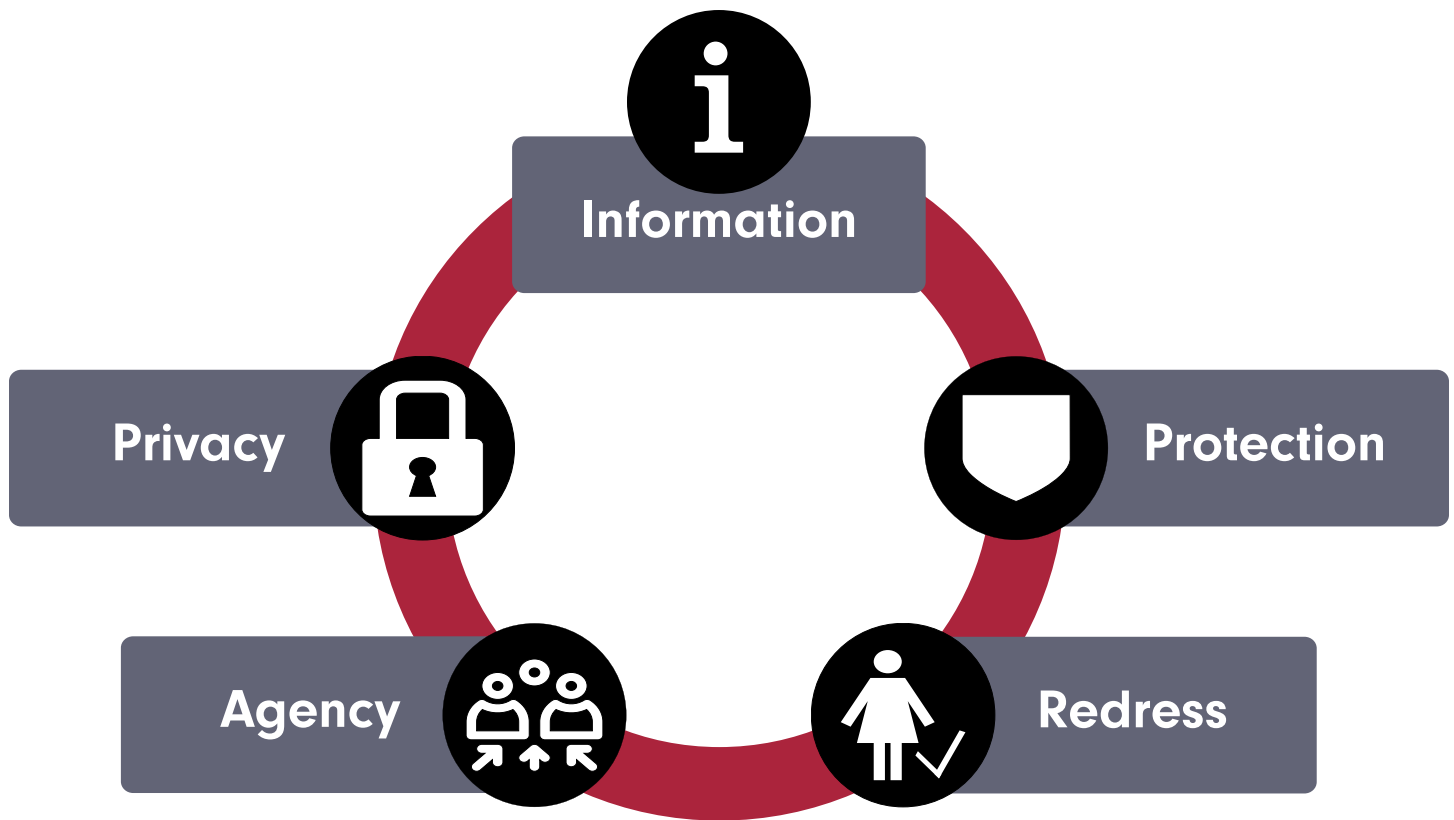
A1. The Right to Information

A2. The Right to Protection

A3. The Right to Data Privacy and Security

A4. The Right to Data Agency

A5. The Right to Redress and Rectification



Preamble

Data is, formally, a collection of symbols which function as a representation of information or knowledge. The term **raw data** is often used with two different meanings, the first being uncleaned data, that is, data that has been collected in an uncontrolled environment, and unprocessed data, which is collected data that has not been processed in such a way as to make it suitable for decision making. Colloquially, and in the humanitarian context, data is usually thought of solely in the machine readable or digital sense. For the purposes of the Signal Code, we use the term data to encompass information both in its analog and digital representations. Where it is necessary to address data solely in its digital representation, we refer to it as **digital data**.

Humanitarian action adheres to the core humanitarian principles of impartiality, neutrality, independence, and humanity, as well as respect for international humanitarian and human rights law. These foundational principles are enshrined within core humanitarian doctrine, particularly the Red Cross/NGO Code of Conduct¹ and the Humanitarian Charter.² Together, these principles establish a duty of care for populations affected by the actions of humanitarian actors and impose adherence to a standard of reasonable care for those engaged in humanitarian action.

Engagement in HIAs, including the use of data and ICTs, must be consistent with these foundational principles and respect the human rights of crisis-affected people to be considered “humanitarian.” In addition to offering potential benefits to those affected by crisis, HIAs, including the use of ICTs, can cause harm to the safety, wellbeing, and the realization of the human rights of crisis-affected people. Absent a clear understanding of which rights apply to this context, the utilization of new technologies, and in particular experimental applications of these technologies, may be more likely to harm communities and violate the fundamental human rights of individuals.

The Signal Code is based on the application of the UDHR, the Nuremberg Code, the Geneva Conventions, and other instruments of customary international law related to HIAs and the use of ICTs by crisis affected-populations and by humanitarians on their behalf. The fundamental human rights undergirding this Code are the rights to life, liberty, and security; the protection of privacy; freedom of expression; and the right to share in scientific advancement and its benefits as expressed in Articles 3, 12, 19, and 27 of the UDHR.³

The Signal Code asserts that all people have fundamental rights to access, transmit, and benefit from information

1. International Federation of the Red Cross and Red Crescent and International Committee of the Red Cross, “The Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief,” 1994, <http://www.ifrc.org/Global/Publications/disasters/code-of-conduct/code-english.pdf>.
2. The Sphere Project, *Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*.
3. United Nations General Assembly, “Universal Declaration of Human Rights,” *United Nations General Assembly Resolutions* 217 A, no. III (December 10, 1948): 71–79.

as a basic humanitarian need; to be protected from harms that may result from the provision of information during crisis; to have a reasonable expectation of privacy and data security; to have agency over how their data is collected and used; and to seek redress and rectification when data pertaining to them causes harm or is inaccurate.

These rights are found to apply specifically to the access, collection, generation, processing, use, treatment, and transmission of information, including data, during humanitarian crises. These rights are also found herein to be interrelated and interdependent. To realize any of these rights individually requires realization of all of these rights in concert.

These rights are found to apply to all phases of the data lifecycle—before, during, and after the collection, processing, transmission, storage, or release of data. These rights are also found to be elastic, meaning that they apply to new technologies and scenarios that have not yet been identified or encountered by current practice and theory.

No right herein may be used to abridge any other right. Nothing in this code may be interpreted as giving any state, group, or person the right to engage in any activity or perform any act that destroys the rights described herein.

The five human rights that exist specific to information and HIAs during humanitarian crises are the following:

The Signal Code

The Right to Protection

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights. Populations affected by crises, in particular armed conflict and other violent situations, are fundamentally vulnerable. HIAs have the potential to cause and magnify unique types of risks and harms that increase the vulnerability of these at-risk populations, especially by the mishandling of sensitive data.



The Right to Information

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.



The Right to Privacy and Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.



The Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII). Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.



The Right to Rectification and Redress

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.



**HARVARD
HUMANITARIAN
INITIATIVE**

A1. The Right to Information

The right to access, generate, communicate, and benefit from information during crisis

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

Information, including the means to generate, access, acquire, transmit and benefit from it, must be treated as a humanitarian necessity for the survival and well-being of crisis-affected populations by all actors at all times. Accordingly, information in the context of HIAs should be treated as equal in importance to other forms of humanitarian assistance such as food, water, shelter, physical protection, and medicine, and their equitable delivery should be treated as a core part of fulfilling the humanitarian imperative. The right to information is also critical for the recognition that affected persons and communities are agents of their own protection.

Individuals, organizations, and communities engaged in HIAs, including the systems, processes, and infrastructure they employ as part of these activities, should be afforded protection by all actors. This protection should be equal to the protection afforded to other forms of humanitarian assistance under international human rights standards and humanitarian law. HIAs include efforts by affected populations to request assistance from humanitarian actors and to communicate amongst their own communities, regardless of where they are located and the nature of the crisis.

A2. The Right to Protection

The right to protection from threats and harms resulting from the use of ICTs and data during crisis

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights.

Populations affected by crises, in particular armed conflict and other violent situations, are fundamentally vulnerable. HIAs have the potential to cause and magnify unique types of risks and harms that increase the vulnerability of these at-risk populations, especially by the mishandling of sensitive data.

These unique types of risks and harms include, though are not limited to: gross negligence, including lack of necessary technical capacity or expertise; increasing the ability of actors to target specific populations and individuals for attack; marginalizing specific populations; eroding trust between humanitarian actors and crisis-affected populations; and contributing to the potential exploitation of crisis-affected populations. These risks increase significantly in complex emergencies and conflict settings because of the threat of violence against vulnerable populations by state and non-state actors.

Exploitation as a result of HIAs can be defined as actions that include, though are not limited to: corruption, fraud, and price gouging; non-consensual experimentation; the sale or monetization of a population's data without their consent; and the intentional misuse of data to disproportionately benefit or disadvantage a specific group.

A3. The Right to Privacy and Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.

Individuals whose data are collected as part of HIAs have a right to expect that their data are only collected for specified and legitimate humanitarian assistance-related purposes. This right ensures that these data are:

1. processed fairly and lawfully, and not further processed in a way incompatible with that purpose;
2. adequate, relevant, and not excessive in relation to that purpose;
3. accurate and, where necessary, kept up-to-date; and
4. not kept longer than necessary to achieve the stated purpose under which informed consent and/or participation was obtained.

Data encompassed by this right can include both data traditionally defined as personally identifiable information (PII) and any other forms of data that may lead to the identification of individuals or groups of individuals. This right also mandates that care be taken to identify the specific vulnerabilities of persons or groups in relation to particular threats, and to afford them additional protections for the privacy and security of their data as required.

A4. The Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII).⁴ Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.

The right to data agency encompasses the right to protection from non-consensual experimentation, and includes the concepts of informed consent, participation, and notification of data collection and uses.

Everyone has the right to protection from non-consensual experimentation. This right is explicitly articulated in Article 7 of the ICCPR, and is necessary for the realization^{5,6} of both Article 1 of the UDHR, which provides that “All human beings are born free and equal in dignity and rights,” and Article 7 of the Declaration of Helsinki, which states, “Medical research is subject to ethical standards that promote and ensure respect for all human subjects and protect their health and rights.”⁷ As such, everyone has the right to provide voluntary informed consent, consistent with international law and human rights standards, for the use of their PII in all prospective and retrospective applications, including both non-experimental and experimental uses. Informed consent for the acquisition and use of PII is required for the realization of the right to protection from harm resulting from the use of ICTs and data. Populations affected by crises should be extended additional safeguards

4. Nathaniel Raymond, “Beyond ‘Do No Harm’ and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society’s Use of Data,” in *Group Privacy: New Challenges of Data Technologies*, ed. Linnet Taylor, Luciano Floridi, and Bart van der Sloot (Springer International Publishing, 2016), doi:10.1007/978-3-319-46608-8.
5. UNESCO, “Explanatory Memorandum On The Elaboration Of The Preliminary Draft Declaration On Universal Norms On Bioethics,” in *First Intergovernmental Meeting of Experts Aimed at Finalizing a Draft Declaration on Universal Norms on Bioethics* (Paris, 2005), 5, <http://unesdoc.unesco.org/images/0013/001390/139024e.pdf>.
6. UNESCO, “Records of the General Conference,” in *Resolution 15 Adopted by the General Conference at Its 33rd Session*, vol. 1 (Paris, 2005), 74–80, <http://unesdoc.unesco.org/images/0014/001428/142825e.pdf#page=80>.
7. World Medical Association, “World Medical Association Declaration of Helsinki Ethical Principles for Medical Research Involving Human Subjects,” June 1964, <http://www.wma.net/en/30publications/10policies/b3/>.

designed to protect vulnerable populations participating in experimentation, including during the informed consent process.

Relatedly, populations affected by crises deserve to be reasonably informed about HIAs, even when the right to informed consent may not apply. This process—separate and distinct from informed consent—constitutes notification and informed participation. Informed participation is the effort to inform populations about how group data, including DII that may include them, will be acquired and used.

Engaging in informed participation seeks to ensure that affected populations may provide input about proposed and ongoing uses of data derived from them or relevant to them. While informed participation about current or future uses of group data may not always be possible, humanitarian actors must always endeavor to solicit informed participation as part of any HIA.



A5. The Right to Redress and Rectification

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.

Individuals subject to HIAs have the right to know if their personal data are being held, by whom, and who has access to their data. Individuals should also have the right, within a reasonable time period and at a reasonable cost, to access personal data about themselves. They should be provided this data in a form intelligible to them, enabling them to verify and challenge the accuracy of data about themselves. In the event that such access needs to be restricted or denied, data managers must provide the individual with clear reasons for the denial of their request.

As part of the right to redress, affected persons and populations have a right to obtain the correction, blockage, and erasure of their data under certain circumstances. Examples of these circumstances may include:

- instances when informed consent applied but was not obtained;
- the infliction of harm as a direct result of HIAs on individuals or groups;
- non-consensual experimentation as part of a HIA;
- negligence leading to a personal data breach or group data breach;
- data are demonstrably inaccurate but unrectifiable; or
- when the means by which data are obtained or processed violates accepted human rights standards.