World Vision

Data Protection, Privacy and Security for Humanitarian & Development Programs

DISCUSSION PAPER

Authors:
Al Lutz, WVI Chief Info Security Officer
Amos Doornbos, WVI HEA Strategy & Systems Director
Anna Kehl, WVI ICT4D Volunteer
Annette E. Ghee, Ph.D., WVI Research & DME Technical Director
Laura DePauw, WVI Sustainable Health Knowledge Management Coordinator

Editor:
Sherrie S. Simms, Ph.D., WVI ICT4D Director

This Discussion Paper has been created to facilitate knowledge exchange and discussion. It is not a formal publication of World Vision International (WVI), has not been edited to official publication standards, and the findings, interpretations and recommendations do not imply an official position on the part of WVI. The research, content and conclusions presented in this paper are those of the authors and do not necessarily reflect the policies or perspectives of WVI.

The electronic version of this document can be accessed at: http://wvi.org/health/ict4d

World Vision is a Christian relief, development and advocacy organisation dedicated to working with children, families and communities to overcome poverty and injustice. Inspired by our Christian values, we are dedicated to working with the world's most vulnerable people. We serve all people regardless of religion, race, ethnicity or gender.

Table of Contents

Strategic Opportunities and Imminent Risks

As the relief and development sector has matured over many decades, Information & Communication Technology for Development (ICT4D) has shifted more recently from innovation to a catalytic tool for attaining target socioeconomic development goals[1]. Practitioners of ICT4D from international and local Non-governmental Organizations (NGOs), civil society organizations, the United Nations (UN) agencies, donor agencies and private sector companies are increasingly aware of the inherent opportunities and risks involved with capturing, analysing and leveraging data about beneficiaries and sub-populations.

> Information & Communication Technology (ICT) is the most powerful new tool we have for solving the world's major challenges—ending poverty and hunger, ensuring universal access to basic services, and making the transition to a low-carbon economy. . . .
> Yet technology by itself is never a solution. It must be properly deployed—directed towards social purposes—and extended to the poor and to remote regions that markets alone will not serve, at least not in a timely way. Put simply, technology must be combined with a will towards the common [global] good. In our era, that means harnessing it to the global objectives embodied by the Millennium Development Goals and Sustainable Development Goals.
>
> Dr. Jeffrey D. Sachs

Crowd-sourced efforts to define and address these opportunities and risks have led to some progress across the ICT4D space and have produced results such as the following definition of *Responsible Data*: "The duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness."[2] In addition, individual agencies, NGOs, donors, private corporations and others[3] have been working to define their own approaches to these issues.

Useful research and recommendations on responsible data have also recently been published by the UN Office for the Coordination of Humanitarian Affairs,[4] and by GovLab at New York University/Centre for Innovation at Leiden University[5]. Yet, there still remains a gap in terms of commonly agreed and utilized principles and standards to ensure a high level of adherence to data protection, privacy and security principles and standards for ICT4D. Given the potentially harmful risks of failing to put in place appropriate safeguards, a collaborative effort in the humanitarian, development and ICT4D sector to further delineate Digital Development Principle 8: Address Privacy & Security[6] is timely and much needed.

Based on Information Technology (IT) industry standards, World Vision International (WVI) has been implementing a Data Protection, Privacy & Security (DPP&S) framework for the last four to five years. This framework is applicable to WVI globally as well as specific ICT4D projects with respect to relevant approaches and safeguards. In order to understand the current landscape of other existing frameworks, regulation, research and compliance, WVI has undertaken a desk research process of these broader global trends and has also documented its implementation of its own framework along with case studies of its approach in humanitarian assistance and health and nutrition.

---

[1] Dr. Jeffrey D. Sachs, *Director of the Earth Institute at Columbia University and Special Advisor to United Nations Secretary-General Ban Ki-moon on the Sustainable Development Goals.* How Information & Communications Technology can Accelerate Action on the Sustainable Development Goals, 2016.
[2] The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment, Responsible Data Forum, 2016. https://responsibledata.io/resources/handbook/assets/pdf/responsible-data-handbook.pdf
[3] U.N. Global Pulse, Oxfam, Catholic Relief Services, MasterCard, Visa, DFID/UKAid, UN OCHA & others
[4] Building Data Responsibility Into Humanitarian Action. U.N. OCHA, May 2016. https://docs.unocha.org/sites/dms/Documents/TB18_Data%20Responsibility_Online.pdf
[5] Mapping and Comparing Responsible Data Approaches, GovLab, New York University & Centre for Innovation, Leiden University. June 2016. http://www.thegovlab.org/static/files/publications/ocha.pdf
[6] Digital Impact Alliance – Digital Development Principle 8: http://digitalprinciples.org/address-privacy-security/

Existing guidelines, regulation & frameworks relevant to ICT4D

There are a number of key frameworks that are relevant to addressing Digital Development Principle 8. While all provide some challenge in the context of implementation of humanitarian, development and ICT4D programmes, they are important benchmarks that should be assessed and considered for implementation.

The **Organization for Economic Cooperation and Development (OECD) privacy guidelines** were last updated in 2013 to provide a risk-management approach as well as a discussion on the importance of developing international interoperability in ensuring privacy. OECD's members are given a framework of guidelines as well as suggestions for implementation. Both the public and private sectors in these nations are responsible for providing:

- limits to the collection of data;
- data quality assurance;
- purpose specification of data at time of collection;
- limitation of data use to specified purpose;
- assurance of security safeguards;
- openness about practice, policies, and developments regarding the data;
- specified set of rights for the individuals from whom data is collected;
- accountability of the data controller.[7]

There are guidelines for international data flow, requiring restrictions to reflect legitimate risks and encouraging low restrictions on data flow between member nations. Privacy management programmes, data security breach notification systems, and national privacy strategies are addressed as well.[8] It is important to note that the member nations of OECD are primarily wealthy, technologically advanced nations that have been able to put in place solid regulatory frameworks. While only six of the thirty-five members are from outside of Europe and North America, OECD also has agreements and partnerships with many non-member nations which may not have regulatory frameworks in place.

Two critical benchmarks that must be considered when evaluating existing data protection, privacy, and security standards are the **United States' Health Insurance Portability and Accountability Act of 1996 (HIPAA)** regulations, and the **European Union's General Data Protection Regulation (GDPR)**, which will replace the current Data Protection Directive starting May 2018. The GDPR has much more stringent regulations than HIPAA, and organisations in developed countries as well are concerned about their ability to meet the GDPR requirements.

HIPAA includes four rules known as the "Privacy Rule", the "Security Rule", the "Enforcement Rule", and the "Omnibus Rule".[9] The Privacy Rule and Security Rule are most relevant to ICT4D, as they address protection of individually identifiable data and protection of electronic health data.

The Privacy Rule protects individually identifiable information, mandating disclosure of what is the "minimum necessary" and limiting disclosure of the following:

1. individual identified by the information;
2. the entity's own treatment, payment, and healthcare operations;
3. uses and disclosures to which the individual has the option to agree or object;
4. incidental use and disclosure;

[7] The OECD Privacy Framework, OECD, 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[8] "2013 OECD Privacy Guidelines," OECD. Accessed April 11, 2017, https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.
[9] "HIPAA For Professionals," Office for Civil Rights, US Department of Health and Human Services. Accessed March 31, 2017, https://www.hhs.gov/hipaa/for-professionals/index.html.

5. public interest and benefit activities;
6. limited data sets which have been de-identified.

Individuals have the right to view their data and amend it as needed; the right to be notified when and to whom individually identifiable data has been disclosed; and the right to request restricted access of their data to different entities.[10]

The Security Rule is designed "to protect the privacy of individuals' health information while allowing covered entities[11] to adopt new technologies to improve the quality and efficiency of patient care."[12] Regarding electronically-Protected Health Information (e-PHI), entities must:

- ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- identify and protect against reasonably anticipated threats to the security or integrity of the information;
- protect against reasonably anticipated, impermissible uses or disclosures;
- ensure compliance by their workforce.

Procedures for doing so are not specified; however, the Security Rule does provide some guidance on crucial considerations for creating procedures. Entities are required to perform ongoing risk analysis and provide a specified set of physical, technical, and administrative safeguards.

Like the European Union's current Data Protection Directive, the new **General Data Protection Regulation (GDPR)** places conditions on processing any kind of personal data. For "lawful processing" to occur, a legal basis for the use of that data must be documented, and it cannot violate eight key individual rights, as discussed below.[13] The GDPR has specific policies for the protection of children's rights as well, requiring that children must be able to understand the privacy notices, and that online services offered for children may only process data with a guardian's consent unless they are preventative or counselling services.

Individual rights according to the GDPR include:

1. the right to be informed
2. the right of access
3. the right to rectification
4. the right to erasure
5. the right to restrict processing
6. the right to data portability
7. the right to object
8. rights in relation to automated decision making and profiling.[14]

The most noteworthy difference between the current Data Protection Directive and the new GDPR is an emphasis on accountability. Not only must organisations adhere to the GDPR, but they must set up their own governance system to demonstrate adherence and keep records. While there is a list of what the records must

[10] "Summary of the HIPAA Privacy Rule," Office for Civil Rights, US Department of Health and Human Services. March 2005. Accessed March 31, 2017, https://www.hhs.gov/sites/default/files/privacysummary.pdf.
[11] Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.
[12] Summary of the HIPAA Security Rule," Office for Civil Rights, US Department of Health and Human Services. Accessed March 31, 2017, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
[13] "Key Areas to Consider," Overview of the GDPR, Information Commissioner's Office, licensed under the Open Government License. Accessed March 31, 2017, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/.
[14] "Individual's Rights," Overview of the GDPR, Information Commissioner's Office, licensed under the Open Government License. Accessed March 31, 2017, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/.

document, there is not a certain structure of governance that must be used across the board. Performing data protection impact assessments is strongly encouraged though not required.[15]

The DLA Piper law firm has found that few organisations currently meet the requirements and thus suggests that they focus on meeting these requirements even before the GDPR begins to be enforced to ensure that they fully comply by May 2018.[16] This is particularly relevant for those in the healthcare and life sciences sector, as they score the lowest on compliance with the new standards at the moment.

The **Asia Pacific Economic Cooperation (APEC) Privacy Framework**, created to support electronic commerce, seeks to protect information through a flexible approach that will ensure privacy but not create unnecessary barriers to information exchange.[17] The framework's privacy principles are as follows:

1. Preventing harm: Design personal information protections with the goal of preventing harm.
2. Notice: Either before, at the time of, or as soon as possible after information collection, individuals must know:
    a) that their information is being collected;
    b) why it is being collected;
    c) to whom the information will potentially be disclosed;
    d) the identity of the personal information controller and how to contact them;
    e) options available for limiting the disclosure of their information.
3. Collection limitation: Only information relevant to the purpose of collection may be collected, and collection methods must be legal, fair, and with notice to the individual from whom the data is collected.
4. Uses of personal information: Personal information may only be used for the stated purpose for which it was collected and other closely related purposes unless the individual gives consent. The information must only be used to provide a product or service requested by the individual, or by the authority of law.
5. Choice: Individuals must be provided with understandable, accessible, and affordable ways to exercise choice over the collection, use, and disclosure of their information.
6. Integrity of personal information: Personal information must be accurate, complete, and as up-to-date as is necessary for the use of the information.
7. Security safeguards: Personal information controllers must protect personal information with safeguards proportional to the level and severity of risk.
8. Access and correction: Individuals must be able to access and challenge the accuracy of the information that the personal information controller holds regarding them, as well as have the information corrected or deleted if appropriate. If deemed not appropriate, the individual must be provided with reasons why.
9. Accountability: The personal information controller must be accountable for complying with the principles above.

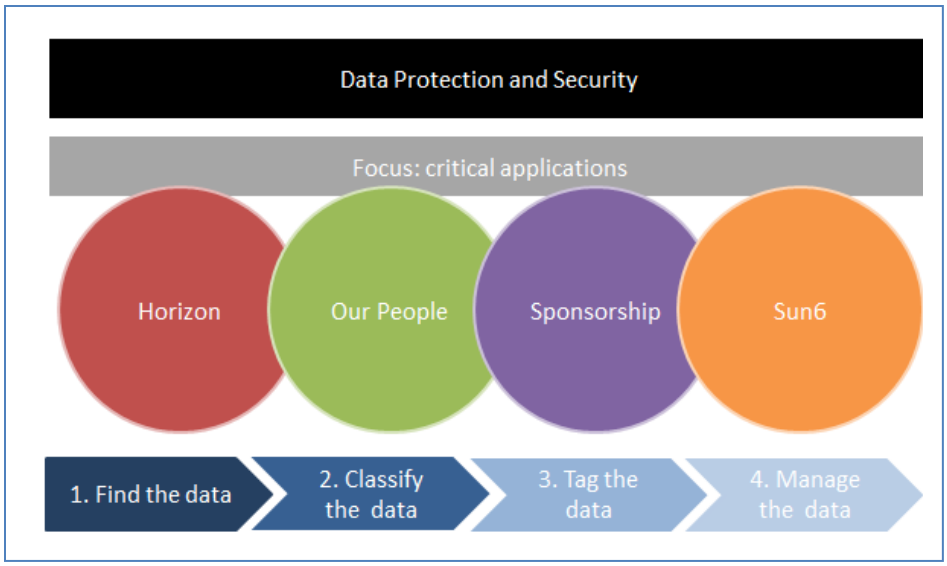
[15] "Overview of the GDPR," Information Commissioner's Office, licensed under the Open Government License. Accessed March 31, 2017, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.
[16] Global Data Privacy Snapshot 2017: How does your organization compare? DLA Piper. https://www.dlapiper.com/~/media/Files/Insights/Publications/2017/01/DLA%20Piper%20Whitepaper.pdf.
[17] APEC Privacy Framework, APEC Secretariat, 2005. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

WVI Data Protection, Privacy & Security Framework

Inherent within World Vision's portfolio, data protection, privacy and security are specific concerns. We have been using digital technology in our humanitarian and development work to amplify the impact and quality of our programming for many years, with ICT4D project work documented as early as 2003. We currently use digital technology in our disaster management, health, nutrition, food assistance, education, advocacy, water and sanitation, agriculture and economic development work. Because of this breadth of scope, safe data standards for our donors, beneficiaries, employees and partners is a serious concern. Effort has been undertaken in recent years to establish World Vision's framework for information security and privacy, and has wrestled with what data security should look like in humanitarian contexts. However, as ICT4D is a new area in the development world, there is still a lot of work to be done to arrive at consensus on global standards for data protection, privacy and security.

Information security and privacy

World Vision believes that in order to assure sensitive information is both secure and private, all information security, privacy and legal stakeholders need to be in alignment. World Vision has made strides in the past few years in bringing the privacy and information security groups together structurally with close linkages to the World Vision Legal team. This, combined with the development of global policies and assessment processes, is strengthening World Vision's information security and privacy posture.



When looking at data protection and security issues, World Vision is targeting a four-step process: *finding the data* (primarily structured data); *classifying the data* (public, private, confidential, etc.); *tagging the data* (based on how sensitive it is); and *managing the data*. This process is hard to do well but World Vision focuses on its most critical applications:

- *Horizon* (World Vision's integrated system with design, monitoring and evaluation, project budgeting, sponsorship monitoring, child well-being outcome reporting and rich media capacities);
- *Our People* (World Vision's centralized employee HR system);
- *Sponsorship* (World Vision's sponsored-child database);
- *Sun6* (World Vision Partnership's global financial system).

When looking at risk, the Enterprise Risk Management (ERM) team works closely with the Information Security team to assure that both groups are looking at and classifying risk from the same vantage point. ERM looks at World Vision's global functions, weights the risks of each organisational function, and creates a normalized list of the top ten organisational risks. These risks and corresponding risk categories have been globally aligned. Currently, fundraising offices (internally referred to as Support Offices [SOs]), have their own risk systems into which WVI provides input, however, future plans include integrating these systems.

Current policies in place

World Vision's development of global information security and privacy policies has been a work in progress over various years. In recent years, Information Security, in conjunction with Legal and the ERM, leveraged the International Organisation for Standardisation (ISO) to develop a set of policies based on global standards. Through this process, three policies were developed which apply to all World Vision entities, including microfinance institutions:

- *Partnership Policy on Global Data Protection and Privacy:* This policy provides an overarching framework for global data protection and privacy at World Vision, documenting the data protection and privacy principles and policies required to ensure there is consistency in data protection and privacy, compliance with applicable data protection/data privacy law, good practice, protection of Personally Identifiable Information (PII), and minimization of risks of regulatory compliance failures and reputational damage for the World Vision Partnership. It is the primary policy under which all other data protection and privacy related policies reside.
- *Partnership Policy on Information Security:* This policy provides an overarching framework for information security at World Vision, documenting the information security principles and policies required to ensure confidentiality, integrity and availability of World Vision's assets, information, data and IT services. It is the primary policy under which all other technical and security related policies reside.
- *Management Policy on Information Security:* This policy targets and addresses global information security functions, issues, and concerns for the World Vision Partnership. It is supported by and is in alignment with the board-approved Partnership Policy on Information Security. Offices can add additional detail or make them more stringent, but their policies must meet the minimum standard of this policy. The next step will be to reconcile current policies with this policy.

A Management Policy on Global Protection and Privacy, and a set of Data Protection and Privacy Security Standards, have been drafted and are currently in a review cycle. These policies are a good start and serve as a baseline standard for all offices.

Enforcement mechanisms

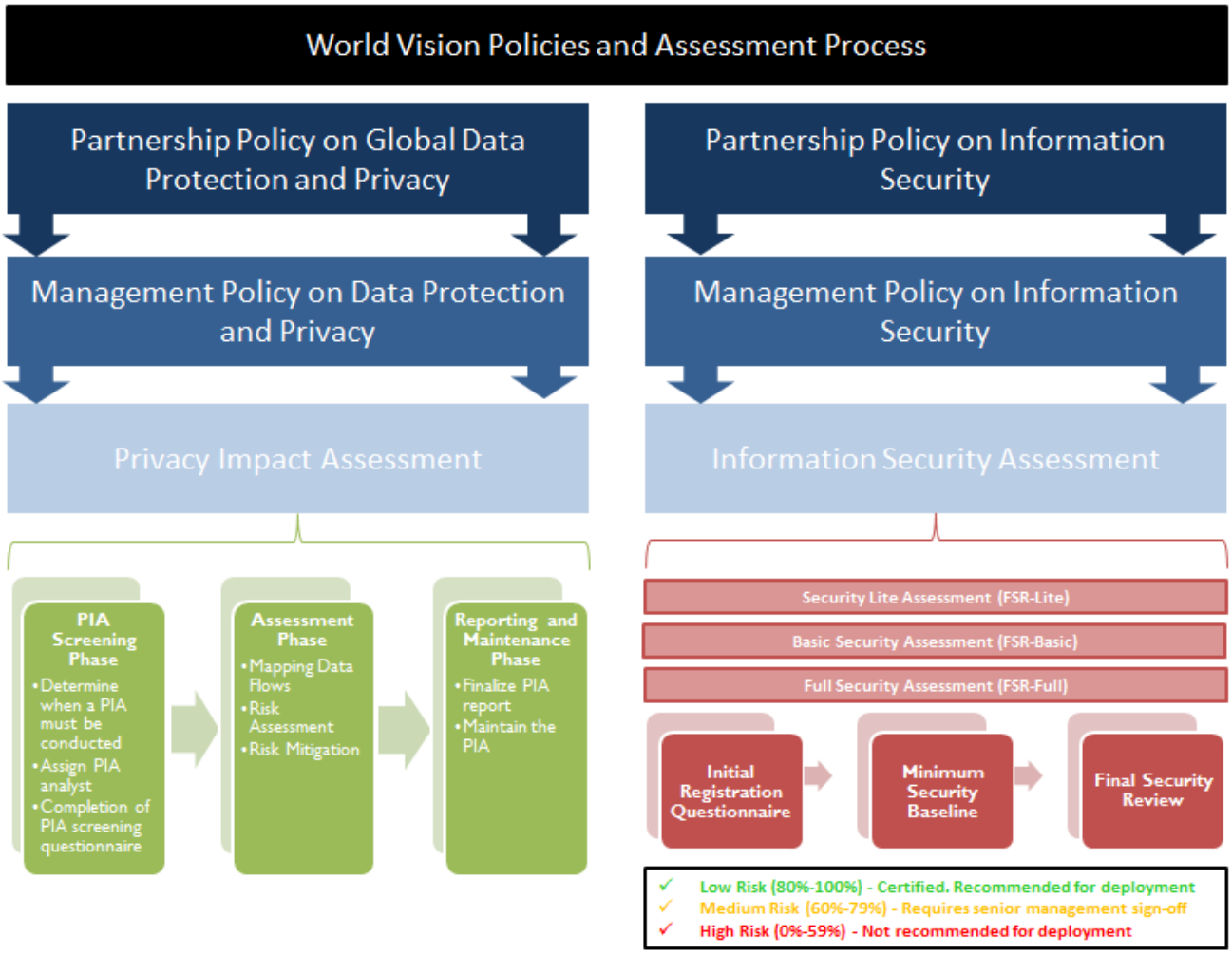
Developing policies is an important step, but enforcement can often be difficult. Current methods include the Staff Training for Information Security Awareness, designed to equip staff to take responsibility for safeguarding organisational data and information from unauthorised users, to recognise potential security risks, and to be able to report incidents immediately. Online training combined with learning reinforcements and phishing assessments help reinforce learnings. Plans are in development to create Staff Training for Global Data Protection and Privacy.

Information security assessment process

In addition to policy, World Vision has developed project integration information Final Security Review (FSR) assessments. In order to assure that assessments are fit for purpose, World Vision carries out three levels of assessments:

1. *Security Lite Assessment* (FSR-Lite): used to assess Commercial Off-the-Shelf (COTS) applications, cloud services, external web hosting, and external service providers;
2. *Basic Security Assessment* (FSR-Basic): used to assess minor releases containing approved changes, new functionality, or new components for existing application, service, or system;

3. *Full Security Assessment* (FSR-Full): used to assess projects introducing major releases, new versions, or new designs for major partnership-wide applications/services (e.g., Sponsorship, Horizon, Financial Systems; Our People).



Source: Department of Information Security, World Vision International

Once the level of approach is determined, the below three-step security assessment approach is applied:

1. *Initial registration questionnaire:* covering the policies, perimeter, network, servers, desktop/mobile, apps and data;
2. *Minimum security baseline:* includes policy review attestation and certifications, Minimum Security Baseline (MSB) perimeter security, architecture review, vulnerability scanning (Qualys©[18]), security configuration wizard, application code review, and MSB data management;
3. *Final security review:* through this process, a final assessment score is determined. Low risk (80%-100%) are certified and recommended for deployment, medium risk (60%-79%) requires senior management sign-off, and finally high risk (0%-59%) are not recommended for deployment.

[18] Qualys© Vulnerability Management. https://www.qualys.com/suite/vulnerability-management/

Post-deployment there are third-party penetration assessments from the big four tier 1 applications (*Horizon, Our People, Sponsorship,* and *Sun6)* and vulnerability remediation to assure continued information security of the project.

Looking ahead

Going forward, World Vision has more to do but we have great work to build upon. We are working to standardise the policy framework as we currently have some policies that are not linked. Both the Management Policy on Global Protection and Privacy and Data Protection and Privacy Security Standards need to be approved by senior leadership. Privacy Awareness Training is needed for all WVIT staff and, finally, Privacy Impact Assessments for *Horizon, Our People, Sponsorship,* and *Sun6.*

Ethical Considerations

Many of the global privacy and security standards described thus far are based on an ethical framework. These frameworks generally include the values of preventing harm, ensuring privacy, maintaining confidentiality during disclosure, and ensuring that the benefits of data collection outweigh the risks; therefore existing standards worldwide have ethical considerations embedded within them.

The United States Federal Trade Commission's "Fair Information Practice Principles"[19] are often referenced as a strong set of ethical guidelines and have been used as a model by many organisations and governments when creating their own data protection standards. Many U.S. laws are based upon these as well. The principles are as follows:

1. An individual must be notified of privacy practices before data is collected.
2. Consent to the specific use of the data being collected must be given by the individual, and consent may be given or removed at any point.
3. The individual must be able to view and correct their data at any time.
4. Data integrity must be kept and security measures and safeguards must be present.
5. There must be a system in place to enforce compliance to the above standards that allows the individual to cite grievances against the organisation collecting the data.[20]

Critics point out that there is no principle requiring a governing authority, leading to too much reliance on self-regulation.

In May of 2015, UN Global Pulse facilitated a workshop titled "Improving Data Privacy & Security in ICT4D" at the UN Headquarters in New York. At this workshop, a number of ethical issues were addressed with emphasis on:

1. the need to obtain consent from those individuals from whom data is obtained;
2. the importance and current lack of privacy risk assessments in any programme or project collecting identifiable information;
3. the reality of the insecure nature of data transfer and the importance of creating secure mechanisms by which de-identified information can be disclosed;
4. the need for transparency, particularly as it comes to building trust with communities and individuals.[21]

[19] https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission
[20] "Fair Information Practice Principles," CIPPGuide and Jon-Michael C. Brook, January 2010. Accessed March 28, 2017, https://www.cippguide.org/2010/01/18/fair-information-practices-principles/.
[21] Improving Data Privacy & Security in ICT4D: A Workshop on Principle 8 of the Digital Development Principles, meeting report, U.N. Global Pulse 2015. http://www.unglobalpulse.org/sites/default/files/Data%20Privacy%20and%20Security%20in%20ICT4D%20-%20conference%20report%20layout%20-%20FINAL.pdf

In respecting these issues, we face unique challenges in a humanitarian setting. The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) policy paper "Humanitarianism in the Cyberwarfare Age" discusses the challenges of informed consent in a crisis situation.[22] Those requiring medical attention may be unable to give consent due to their physical condition. When it comes to situations where minutes taken to get consent could mean life or death, saving lives takes precedent.

At the start of a crisis, organisations may not be sure yet how data will be used, making it difficult to inform individuals properly, and even when a statement about disclosure and use is given, those with low literacy levels in the language that the statement is written in still may not be able to properly give informed consent. Furthermore, beneficiaries may consent to actions that, in a non-crisis setting, they would never condone. It is difficult to see a way to eliminate the potential for coercion created by the crisis itself. "Absolute protection would make humanitarian response impractical by not allowing the collection of any information, while the public listing of personal details would likewise endanger lives," concludes OCHA. "Clearly, the imperative to save lives under difficult circumstances must be balanced with the responsibility to do no harm."

OCHA's policy paper cites risk assessments as an integral starting point in data collection in humanitarian crises, and UN Global Pulse's workshop had a breakout session to brainstorm major factors in creating a benefits, harms, and risks frameworks. Performing a risk assessment gives humanitarian workers who are not data security experts a concrete way to consider if, and to what degree, the benefits outweigh the risks and harms. UN Global Pulse is currently developing a two-phase assessment tool for humanitarian projects; the initial assessment tool has been completed and can be downloaded from their website.[23] However, a lack of resources such as staff and funding is common for humanitarian organisations, and this can create a barrier to performing risk assessments.

Any time data is transferred there is risk of a security breach. A joint effort between NetHope and Mastercard revealed that many humanitarian professionals do not consider there to be a high risk of a security breach.[24] Thus, they do not recognise the importance of de-identifying information and creating secure mechanisms to transfer data as needed, and they do not consider creating secure mechanisms for data transfer to be a priority. Donors often feel the same way and would rather their money go somewhere other than to the development of internal security measures.[25] Even the communities from whom data is collected may not fully understand the importance of data security, as privacy can be considered a Western value and risk is weighed differently by different cultures.[26]

In fact, there are a number of high risks involved when considering humanitarian data. OCHA lists political attacks, attacks on marginalised community members who receive aid, attacks on humanitarian partners, and criminal activity and fraud as the most pressing risks for the humanitarian sector.[27] The U.S. Department of State's Overseas Security Advisory Council (OSAC) has said that "humanitarian missions are more vulnerable to network intrusions given a lack of resources for cybersecurity programmes, and threat actors increasingly view humanitarian organisations as an easy target."[28] These risks are all ethical considerations that must be taken into account, as any of these types of breaches could violate privacy and cause harm.

---

[22] Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies, OCHA, October 2014. http://digitalprinciples.org/wp-content/uploads/2015/12/Humanitarianism-in-the-Cyberwarfare-Age-OCHA-Policy-Paper-11.pdf

[23] U.N. Global Pulse, 'Data Innovation Risk Assessment Tool,' 2016. http://www.unglobalpulse.org/privacy/tools

[24] "Think Responsibly: How We're Helping NGOs Protect Humanitarian Data," Paul Musser and David Goodman, Agenda for Humanity, 2016. Accessed April 11, 2017, http://www.agendaforhumanity.org/news-details/5805.

[25] Improving Data Privacy & Security in ICT4D: A Workshop on Principle 8 of the Digital Development Principles, meeting report, U.N. Global Pulse 2015.

[26] "The Ongoing Challenge of Protecting Privacy in Digital Development," ICT Works, April 2016. Accessed Aprip 11, 2017, http://www.ictworks.org/2016/04/18/the-ongoing-challenge-of-protecting-privacy-in-digital-development/.

[27] Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies, OCHA, October 2014. http://digitalprinciples.org/wp-content/uploads/2015/12/Humanitarianism-in-the-Cyberwarfare-Age-OCHA-Policy-Paper-11.pdf

[28] "Think Responsibly: How We're Helping NGOs Protect Humanitarian Data," Paul Musser and David Goodman, Agenda for Humanity, 2016. Accessed April 11, 2017, http://www.agendaforhumanity.org/news-details/5805.

Transparency is vital when it comes to ethical humanitarian work. World Vision has a stated policy that the data collected from a community belongs to the community. World Vision's Open Information Policy explains that "if external stakeholders are to have confidence in us, they need to be sure that World Vision will 'disclose' relevant information when this is appropriate to enable them to make valid decisions about World Vision and our work."[29] This can be difficult when data is stored and accessed online, particularly if it written in a language other than that read by those from whom the data was collected. OCHA suggests that organisations find ways for these communities to exercise their right to freely access accurate, updated data, even if it requires a "low-tech" solution. They should also be reminded of the privacy policy and given ways to submit complaints and corrections to the data.

World Vision Experience

Issues surrounding data protection and security exist everywhere and working in the humanitarian sector is no exception. It can be easy to jump to technology as a solution, but data protection is essentially a people issue. It involves the data of *people*, collected by *people*, through processes managed by *people*. Personally Identifiable Information (PII), data about an individual's vulnerabilities, and sensitive data have been collected by the NGO community for decades and often haven't been properly stored and vigilantly shared. Now that an increasing volume of data is being captured digitally, the risk of exposure is increasing exponentially.

World Vision's approach to data protection and security in humanitarian and development contexts can be implemented in one of two ways: we can attempt to lock down and control everything, or we can work together to enable others to make wise choices and implement projects as securely as possible. Both options require clear decisions and investment and speak to the type of organisation World Vison wants to be. In line with our core values[30], World Vision strives to work together with partners for the benefit of our beneficiaries. In order to address data protection ethical concerns while delivering community-based programming or mounting a humanitarian response, understanding the issues that practitioners face is essential.

Effectively working within a regulatory environment

Legal and regulatory frameworks governing data security and privacy are varied as one looks across the globe. However, general privacy protections consistent with human rights principles are commonly in place. In the health sector WHO has reported that 73 of 116 member states have defined national digital health strategies[31] which typically take data security and privacy as well as ethics into consideration. Yet, there are worrying signs that implementation of these policies may fall short. A recent survey examined current practice related to electronic reproductive and maternal and child health registries and revealed data security safeguards and support for core privacy principles were inadequate, despite having protective legislation in place[32]. Given our collective mandate to harmonize with national information systems, understanding and working within these policy contexts are at the heart of sustainable ICT4D.

In the health sphere, our recent experience suggests that there are varying levels of capability of mHealth project teams to effectively support government counterparts and address gaps in legal and regulatory frameworks, contribute to policy development and augment its implementation. The most effective working relationships are characterized by teams using well-developed partnering competencies with balanced participation from both health and IT professionals through informal engagement mechanisms (advisory or technical boards/committees, policy development working groups and active participation at consensus building events).

[29] "Implementing the WVI Open Information Policy," World Vision, July 2013. http://wvi.org/publication/implementing-wvi-open-information-policy.
[30] http://www.wvi.org/vision-and-values-0
[31] http://www.who.int/goe/survey/2015survey/en/
[32] Myhre et al. BMC Pregnancy and Childbirth (2016) 16:279.

Challenges faced when obtaining 'consent'

In the context of a humanitarian response, beneficiaries are frequently asked for information before they receive goods or services. This raises the question whether or not beneficiaries have given true 'consent.' Humanitarian professionals are learning that the practice of obtaining consent falls on a spectrum between informed and uninformed and is a whole we are closer to uninformed consent than we would like to be. Defining what fundamental type of 'consent' beneficiaries must agree to is key:

1. Consent to use the information given for a stated purpose?
2. Consent to share the information with others and with whom for what reason?
3. Who is responsible to decide when and with whom to share the information?
4. How much risk to the beneficiary arises given the nature of the data collected (e.g. involves documentation of a characteristic that is potentially stigmatizing, illegal or otherwise leads to significant problems for that individual should data security be breached)?

We also need to consider the psychological impact of disaster/traumatic events on a person's ability to make decisions. How does this influence the process to obtain consent and in particular is some level of coercion unavoidable?

Multiple uses of data including unintended discrimination

Stakeholders are requesting information on increasing numbers of indicators leading to a growing set of characteristics (e.g. religion, education, wealth, HIV serostatus or other health status, etc.) captured in data sets. These data sets can provide valuable information to help focus programming or a humanitarian response and protect beneficiaries from harm in fragile contexts. But, while data can be used for legitimate inclusive or vulnerability targeting purposes, it can also be used to exclude and even discriminate. In light of this reality, challenging questions are raised:

1. If we decide to use data only for the reason for which it was collected, would this actually result in us sharing *less*?
2. How do we ensure that senior decision-makers are involved in making decisions regarding the use and sharing of data collected for one purpose, but now being considered for use in a new way? And how do we do this while avoiding micro-managing?
3. How do we guide frontline staff to decide when and how to share data with third parties? Data sharing with local or national government is a frequent request, but can extend to other types of partners such as external researchers.

It is important for humanitarian NGOs to determine internally which staff members (or staff levels or roles) need to access which aspects of data. There is likely no staff member who needs to see *all* the data. Further guidance regarding data sharing between agencies and across borders needs to be developed and adapted to a given country context. When sharing data, organizations should take a minimalist approach with third parties by furnishing solely those data elements that meet their needs. This doesn't mean withholding all programme level assessments, monitoring and impact data, but it is important to be more strategic about how and when this information is shared.

In the health sphere on the other hand, open data access is viewed as desirable and harmonization of data standards is a growing trend that greatly facilitates data exchange or true interoperability across data systems. The international community has called for open data standards and put forward proposals to operationalize these using base syntactic and semantic standards. The diversity of national contexts that drive legal and

normative frameworks around data ownership and individual rights has impeded the emergence of a global consensus around safeguards for data privacy and security yet recent progress in this area is encouraging[33].

Issue of data ownership and privacy

Who do we define as the owner of a beneficiary's data? Is World Vision the owner? If so, what does this mean and what responsibility does this demand? What are beneficiary's rights to data? Can a beneficiary walk into one of our offices and see all the data we have about them, who it has been shared with, and then ask for it to be deleted? At this point in time, this is not easily possible. In the future beneficiaries will have much greater control over who has access to their data, but a more organisational and industry change will have to occur before this becomes a reality.

On the other hand, in the health sector, there is a growing trend towards making de-identified data publicly available in the spirit of scientific knowledge sharing and collaboration. This concept is yet to be reconciled with the data ownership issue.

Designing solutions with data security and privacy in mind

The Digital Development Principles initiative and follow on consultation at the global level has highlighted the need for technology developers working in the health sphere to consider data security and privacy when designing solutions. The EU guidance on this mandates that privacy implications of the application have to be considered at each step of the development and wherever the user is given a choice[34].

Use of biometrics

Biometrics (measurement of physical human characteristics e.g., fingerprint, face recognition, etc.) can be used in a variety of different ways. Unfortunately, most NGOs do not have an agency perspective on biometrics and are often being asked to implement the use of biometrics at the insistence of donors. In some narrowly defined cases, 100 percent certainty of individual identification is itself ethically mandated. One such set of circumstances exists with World Vision's collaboration with an Ebola Vaccine Trial in Sierra Leone. In this case, ethical guidance suggests that researchers must confirm administration of a potentially harmful experimental drug to the intended recipient. When large numbers of participants are involved, biometrics can boost confidence and greatly streamline this process.

Just because biometrics or any other technology innovation is possible, it doesn't mean it *should* be used. A use case for biometrics needs to be clarified and World Vision needs to develop its own perspective on its use.

Cash-based programming: challenging us to think differently

In almost every project World Vision implements, we collect, analyse and generate a great deal of data. However, the recent trend towards greater cash-based programming challenges us as an organisation to think differently about the types of data we collect and what we do with the data. As cash-based programmes mature, we are engaging more with formal financial service providers who have standardised and highly regulated systems and processes. To confirm their identity when we deliver cash to beneficiaries through these mechanisms, we often need to collect data that is classified as personally identifiable information (in this case, referred to as "Know Your Customer" or KYC data). Once collected, we often need to share all or part of the data with third parties. It is critical for us to fully understand this process so that we are clear on what data actually *needs* to be shared and what doesn't, to assure that procedures for data sharing comply with global standards and with applicable national policies intended to safeguard the privacy and security of data.

In the humanitarian sphere, ICT solution design must appropriately balance the beneficiary's right to privacy with the need to reduce fraud, or in some cases respond to demands for information in the name of terrorism.

[33] https://ohie.org/2017/03/openhie-values-and-digital-principles/
[34] http://www.who.int/goe/survey/2015survey/en/

Geo-coded data: a unique set of challenges

In several development spheres, the use of geo-coded data has been gathering momentum and has proven its value as a powerful analytic lens and maps can powerfully illustrate complex patterns.

Yet with this powerful tool, concerns regarding data security and privacy arise. This is no more evident than with the Demographic and Health Surveys where techniques have been developed to "de-identify" geo-coded information by introducing a small yet known amount of random spatial displacement to the data such that statistical analyses are minimally affected[35]. World Vision has incorporated geo-coded data collection into some aspects of programming, so far only to capture and track the location of key community resources, for example improved water sources or primary health care facilities. There is the potential to include geocode identifiers at household level yet clear policies in this regard are lacking.

Addressing gaps in policies and guidance

In addition to the *Partnership Policy on Information Security* and the *Partnership Policy on Global Data Protection and Privacy*, World Vision does have several ethical frameworks in place. Guidance governing the collection of routine monitoring information has been recently updated and disseminated:

> *Ethics Quick Reference Guide:* This guide summarises the specific ethical requirements that must be followed when collecting qualitative and quantitative data from children. These requirements are documented in the *World Vision Child Protection Standards* and ensure that our processes do not bring more harm than benefit to children.[36]

Policies that offer guidance pertaining specifically to ethics of data collection in the context of both routine evaluation and more rigorous forms of research are currently being updated.

These frameworks are a good starting point but there is room for improvement, both at a policy level and at a practical implementation guidance level. Some areas for improvement include:

- better and more consistent use of Virtual Private Networks (VPNs);
- reducing file sharing over skype;
- reducing the number of offices using insecure wireless Internet;
- increasing the number databases, hard drives, backups, etc., that are encrypted;
- using password managers to improve the quality of passwords being used and being remembered by staff;
- policy defining when data must be de-identified and delineating levels of permissions to access de-identified data for the purpose of business intelligence and on open access to such datasets;
- practical guidance pertaining to preparation of de-identified datasets, including geocoded data and mechanisms to document when data use agreements are required (e.g. giving external researchers access to data);
- articulation of an agency position on biometrics, telemedicine, point-of-care medical diagnostics and other screening tools, outbreak surveillance and drug and commodity supply chain optimization (especially those managed by community health workers[37]);
- better guidance to help frontline staff understand how to discover country specific laws around data protection/security as well as how to apply these laws;
- consistency in how we manage data sharing and storage, including consideration of:
    - in-country storage of all survey data with personally identifying information in-country through a local database;

[35] http://dhsprogram.com/What-We-Do/GPS-Data-Collection.cfm
[36] http://www.wvi.org/child-protection/publication/protection-girls-and-boys-world-visions-systems-approach
[37] https://peoplecentered.net/2016/05/20/transform-health-services/

- in-country storage in encrypted databases for very sensitive data;
- digital identity and personally identifiable information stored in the cloud behind well managed firewalls.

In addition to internal policies and guidance, there are key industry standards in place that help guide our work, including: International Committee of the Red Cross' Rules on Personal Data Protection; Oxfam's Data Protection Policy; Oxfam's Data Privacy Policy; and Information Commissioner's Office's Privacy in Mobile Apps.

Finally, policies and guidance, regardless of their quality, often find themselves in the information graveyard if they are poorly or infrequently communicated. It is important to constantly communicate our existing policies and work to improve them. Staff must be aware of our policies, their contents and relevance to their work.

Anticipating tomorrow's technology

It is important to remember that as the development and humanitarian response community works to grapple with the consequences of today's new technologies, we must also look to the future. In the humanitarian industry, technologies such as BlockChain[38] are revolutionising the financial services world, but also expanding beyond financial data and will transform the information management space in the next five to ten years. Continued innovations in affordable mobile-enabled medical diagnostics and rapid screening tools are examples of ICT that has the potential to transform work in the health sector.

We must understand these technologies and assess their utility and potential risk to our beneficiaries with regard to information security and privacy while preserving the highest possible ethical standards.

Conclusion

The complexities of the contexts where humanitarian and development agencies operate make it quite difficult to implement a fail-safe approach to data protection, privacy and security in its digital work. At the same time, it is incumbent on this sector to strive toward the highest level of integrity, ethics and technical ability to ensure the strongest possible data protection of vulnerable populations, and particularly children.

Therefore, individual and collective effort of individuals and agencies to further address the complexities and risks is of the utmost importance in mitigating the risks inherent in capturing, storing and analysing beneficiary data. A collective call to action to further define and align with Digital Development Principle 8: Address Privacy & Security would exemplify a key step forward.

[38] https://www.blockchain.com/