Principle: Address Privacy & Security

Overview

Addressing privacy and security in digital development involves careful consideration of which data are collected and how data are acquired, used, stored and shared. Organizations must take measures to minimize collection and to protect confidential information and identities of individuals represented in data sets from unauthorized access and manipulation by third parties. Responsible practices for organizations collecting and using individual data include considering the sensitivities around the data they have collected, being transparent about how data will be collected and used, minimizing the amount of personal identifiable and sensitive information collected, creating and implementing security policies that protect data and uphold individuals' privacy and dignity, and creating an end-of-life policy for post-project data management.

Core Tenets

- **Define data ownership, sovereignty and access before any data are collected or captured.** Determine what local data protection laws and regulations need to be followed, who gets to decide what to do with the data, who is allowed to access or use the data and where data can (or must) be stored.
- **Keep the best interests of end users and individuals whose data are collected at the forefront of your planning for upholding user privacy and ensuring data security and ethical implementation.** This is especially important when implementers work with vulnerable or marginalized communities who may not have had a say in how their data have been collected, used or shared.
- **Perform a risk-benefit analysis of the data being processed** that identifies who benefits and who is at risk. This process may need to be repeated throughout the period of performance as new data are needed, new risks are identified or emerge, or new data-sharing partners are considered.

PROJECT LIFECYCLE GUIDANCE

The following recommendations, tips and resources are drawn from the digital development community to give you options for applying this Principle during each phase of the project or software lifecycle. This guidance is not meant to be exhaustive, but rather should serve as suggested actions that you can take to apply this Principle in your work. If you have other tips, resources or comments to add, please share them with the community at https://forum.digitalprinciples.org/

Principle: Address Privacy & Security

- **Assess the risks** of unauthorized access or leakage of any stored data. Consider the impact this data could have on the individuals if accessed or published maliciously and the risks if data were combined with other data sets.
- **Understand that risks are highly contextualized,** not just to countries but also to communities, populations and periods of time. If working with vulnerable or marginalized communities, what groups might have motivation to acquire your data, how capable are they, and are the information and access controls around the data sufficient?
- **Minimize the collection of personal identifiable information.** Consider how critical personal information is to the project's success and what the consequences would be if those data are exposed to third parties — especially when partnering with users from vulnerable populations, such as minority groups, the disabled, and women and children. Include a risk assessment for collecting personal information.
- **Catalog and track any personal or sensitive information captured throughout the project:** Create a plan for mid- and post-project destruction or secure offline storage of sensitive data, including the review of hard drives, cloud file storage, flash drives, email inboxes and other common sources of data leakages.
- **Be transparent** with individuals whose data are collected by explaining how your initiative will use and protect their data.
- **Obtain informed consent** prior to data collection. It is crucial to ensure that participants understand why their data are being collected, how data are used and shared, and how the participants can access or change the data collected — and that they be given the option to refuse to participate. Participants should be informed of and fully understand the risks related to sharing their data. Consent forms should be written in the local language and easily understood by the individuals whose data are being collected.

"Remember that technical security measures are only as strong as the human users of the technology. Design security that is usable in the contexts where the technology is used."

CLAYTON SIMS, DIMAGI

Principle: Address Privacy & Security

- **Protect data** by adopting best practices for securing and restricting access to data. Examples of best practices include encrypting files, using two-factor authentication, restricting access permissions, storing data on secure servers or secure cloud storage services, and implementing organizational security policies and procedures, including data-sharing agreements with all data-sharing partners.

Upholding these tenets is essential to ensuring ethical implementation of digital development initiatives and avoidance of negative outcomes that may result from security breaches. Following data privacy practices and security safeguards protects the interests of communities, while promoting trust between end users and digital development practitioners. Confidentiality and security of personal data should be maintained with an aim to preserve the dignity and security of the individuals represented.

Analyze & Plan

In this phase, think strategically about which data will be collected and how data will be used throughout the project lifecycle. Determine how sensitive information will be kept confidential and secure during each stage, and weigh the risks of compromised data against the necessity of collecting the data in the first place.

- **Identify which data are critical for the initiative's success, and balance the collection of essential sensitive data with the best interests of individuals.** Be aware that the act of data collection itself may put some high-risk populations in jeopardy. Collect the minimum amount of personal identifiable information and sensitive data; be sure to obtain informed consent using forms and language that are understandable to the individuals whose data are being collected. Consider whether anonymous data sets could be combined to identify specific users and link anonymous confidential data to them.
- **Conduct a risk assessment** to identify internal and external threats to your data, as well as system vulnerabilities. Prioritize the threats or vulnerabilities, considering damage potential, number of affected users, exploitability and reputational

ANALYZE & PLAN

TIPS AND RESOURCES

TIP: Follow best practices for collection and management of private data and sensitive information:

- Obtain informed consent from data owners on the processes employedto access, use and share their personal data.
- Be transparent with individuals whose information is collected about how you will use the data.
- Define mechanisms for individuals to access information about how you are collecting and using their personal data.
- Only collect personal data for specific, fair and justified use.
- Minimize data collection and limit data notation to the essential details.
- Enforce standards and follow best practices for data access, updates and management.

RESOURCE: Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG). https://SAFETAG.org

RESOURCE: The OECD Privacy Framework, Organisation for Economic Co-operation and Development: http://digitalprinciples.org/wp-content/uploads/2015/12/oecd_privacy_framework.pdf

RESOURCE: European Union General Data Protection Regulation (EU GDPR). http://www.eugdpr.org/

RESOURCE: African Union Convention on Cyber Security and Personal Data Protection, African Union. https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

risk. Develop a risk management plan outlining the countermeasures you are taking to address high-priority threats.

- **Consider the ramifications for sustainability and scale** when determining which data to collect. You may need to gather more information to support widespread deployment [http://digitalprinciples.org/build-for-sustainability/] [http://digitalprinciples.org/design-for-scale/].
- **Understand local rules and regulations about data privacy and security, including institutional review board regulations.** Speak with government officials, local leaders, data regulators (such as multinational organizations and hospital administrators) and your users [http://digitalprinciples.org/design-with-the-user/]. Understand the consequences of noncompliance (e.g., fines or sanctions), as well as any negative impact that noncompliance will have on your organization's reputation and the success of the initiative.
- **Plan for oversight capacity.** Assign responsibility for security and risk management to specific individuals, and conduct security awareness and training sessions for data users. Identify and secure stable funding for security measures and oversight.

ANALYZE & PLAN

TIPS AND RESOURCES

RESOURCE: The Hand-Book of the Modern Development Specialist, Responsible Data Forum. https://responsibledata.io/resources/handbook/.

Design & Develop

Plans for data management and security should be created, tested and formalized during this phase. You may also be collecting data to inform the design and development of the digital tools being used in the program.

- **Create a data management plan** before any data collection begins. A data management plan details what you will do with the data during and after your initiative to ensure that data are both accessible and secure. Determine answers to the following questions in your plan:
  - **Data collection:** How much data will be collected, over what period will the data be collected, and who is responsible for data collection, management and security?
  - **Validation and cleaning:** Is the removal of personally identifiable information part of the cleaning process (especially of qualitative data)?
  - **Organization and storage:** How are you documenting and saving your data to be understandable and accessible by others, what file formats and naming conventions are you

DESIGN & DEVELOP

TIPS AND RESOURCES

RESOURCE: Data Management Plan Tool, Stanford Libraries. https://library.stanford.edu/research/data-management-services/data-management-plans/dmptool

RESOURCE: Data Management, Massachusetts Institute of Technology Libraries. https://libraries.mit.edu/data-management/plan/write/

RESOURCE: The Hand-Book of the Modern Development Specialist: Designing a Project, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-01-designing-a-project.html

employing, and what are your storage procedures to ensure that data are secure?

- **Access:** Who has the rights to the data, how will data be shared, how will you protect personal data, and will reuse be allowed?
- **Archiving:** How long will data be stored, how will the data be destroyed when no longer needed, and how will data be made anonymous? Is an open source repository available to store the data or will the data be transferred to another organization?

Align your plan with organizational privacy, security and responsible data management policies and open source community standards, if appropriate. Share your plan with partners, target users and the broader digital development community to promote transparency, accountability and trust. Ensure that the plan is understandable and approachable by these varied stakeholders.

- **Identify team members who will be responsible for data management and security throughout the project lifecycle.** Responsibilities include making changes to the data management plan when the external environment changes, conducting a risk analysis, monitoring data to ensure that they are secure and responding to security breaches, as well as training individuals who will take on ownership of the data if the initiative is transferred.
- **Conduct a regular review of system functions that capture data automatically.** During development, new functions may be added to capture data within the system. Can the initiative justify the need to capture that data, and are there clear policies about how data will be collected, stored, used and destroyed.
- **Develop the digital tool to adhere to current information and physical security standards for protecting personal information.** For example, ensure that the platform your initiative is using can manage user access and permissions for viewing or using data.

Deploy & Implement

During this phase, put the data management plan into operation. Depending on the initiative, you may also be collecting personal information. Regularly communicate which data you're collecting,

DESIGN AND DEVELOP

TIPS AND RESOURCES

- **RESOURCE:** Beyond Data Literacy: Reinventing Community Engagement and Empowerment in the Age of Data, Data-Pop Alliance. http://datapopalliance.org/item/beyond-data-literacy-reinventing-community-engagement-and-empowerment-in-the-age-of-data/.
- **RESOURCE:** Data Innovation Risk Assessment Tool, UN Global Pulse. http://unglobalpulse.org/sites/default/files/Privacy%20Assessment%20Tool%20.pdf
- **RESOURCE:** Girl Safeguarding Policy: Digital Privacy, Security, & Safety Principles & Guidelines, Girl Effect. http://www.girleffect.org/media/3052/gem-girl-safeguarding-policys_19-05-16.pdf.
- **RESOURCE:** Responsible Data Management, Oxfam. http://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management.
- **RESOURCE:** Improving Data Privacy & Data Security in ICT4D: Meeting Report, UN Global Pulse. http://www.unglobalpulse.org/blog/improving-data-privacy-data-security-ict4d-meeting-report

DEPLOY & IMPLEMENT

TIPS AND RESOURCES

- **TIP:** Use a data protection checklist to ensure that your data are secure. You can also use this checklist to develop indicators for monitoring and evaluation of data security and privacy.
  - Are all file cabinets locked and paper records secured?
  - Are computers password protected using strong passwords?
  - Have all study participants been assigned anonymous identification numbers?

Principle: Address Privacy & Security

how the data are being used, how they are being kept secure and who is using the data.

- **Control access to data to maintain integrity and confidentiality.** Create access groups with specific permissions depending on the roles of the users. Default to the minimum permissions possible for most individuals, and enable more permissions (such as read/write access) only for essential users. Set up individual password requirements for all users, and consider using two-factor authentication. Single-factor authentication is when you only have to enter your username and one password to log in to an account. With two-factor authentication you go through an extra step after entering your password, such as getting a verification code sent to the phone number associated with the account via SMS and then entering that code to access the account.
- **Implement countermeasures to priority risks and vulnerabilities.** Continue to conduct regular risk analyses and security audits to identify emergent vulnerabilities. Immediately respond to any security breaches to ensure that negative effects are quickly and easily mitigated, and inform individuals whose data have been breached.
- **In the case of closing out the project, implement the plan for either destroying data or moving data into long-term storage.** Destroy any records that are considered sensitive or are no longer required for future initiatives or evaluation. Inform relevant stakeholders of how data are being managed or destroyed.
- **In the case of scale up or transfer, work with new initiative members or organizations to ensure that they understand and adhere to the established data management plan.** Identify any gaps in security that may arise from scale up or transfer. Work with partners to address the gaps and make necessary updates to the data management plan.

Cross-cutting: Monitor & Evaluate

Continue to follow your data management plan, making updates as needed based on monitoring and evaluation (M&E) findings.

- **Develop a data collection plan based on your M&E plan,** incorporating considerations in the data management plan. Ensure that staff are fully trained to carry out the plan and that

DEPLOY & IMPLEMENT

TIPS AND RESOURCES

- Have all staff members been trained on confidentiality and privacy?
- Are all backup files secured?
- Under what circumstances will data be shared and with whom? How will data be shared in a secure way?
- Are security procedures regularly reviewed and updated?
- Don't keep data on flash drives or other external devices that can easily be lost or stolen.
- Don't use email for sending participant-identifiable information.

RESOURCE: Data Protection, Privacy and Security for Humanitarian & Development Programs, World Vision International. http://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs.

RESOURCE: How to Develop and Implement Responsible Data Policies, MERL Tech. http://merltech.org/how-to-develop-and-implement-responsible-data-policies/.

RESOURCE: The Hand-Book of the Modern Development Specialist: Getting Data, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-02a-getting-data.html.

CROSS-CUTTING:
MONITOR & EVALUATE

TIPS AND RESOURCES

TIP: Proper organization of survey (and other) data rests on the consistent use of identification codes throughout the data collection and entry processes. ID codes help ensure that all information can be traced and linked, no matter the source.

Principle: Address Privacy & Security

all data collectors are trained in research ethics. FHI360 offers a free research ethics training curriculum for international development professionals [https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html].

- **Follow the data organization, storage and access components of your data management plan.** Once your data are collected, ensure that they are securely stored while still being accessible. Consider the following:
  - What is the hierarchy and organization of the file system?
  - Where will the metadata for the file system (including the data management plan) reside?
  - What file naming system will you use?
  - How many copies of files will be stored in the electronic database?
  - Will any of the organization's networking technologies for file storage be used (e.g., a shared drive or cloud storage)?
  - How will data be archived?
  - What formats (e.g., Microsoft Word and PDF) will archived data be saved in?
  - How will archived data be protected (e.g., locked database)?
  - How much file storage space will be necessary? Is it available or will it need to be procured?
- **Pay attention to privacy risks and make data anonymous to remove personally identifiable information.** Use ID codes throughout the data collection and entry process so responses can be tracked without violating confidentiality. This is a particularly important consideration for vulnerable or marginalized populations. Be aware that combining data sets can re-identify individuals.
- **Continue to assess data risks and system vulnerabilities.** Ensure that the risk management plan is fully implemented.
- **Consider wider ethical issues.**
- **Monitor indicators related to data security and privacy.** The data security checklist given in *Deploy & Implement Tips and Resources* provides several potential indicators.

CROSS-CUTTING:
MONITOR & EVALUATE

TIPS AND RESOURCES

- **RESOURCE:** The Hand-Book of the Modern Development Specialist: Sharing Data, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-02c-sharing-data.html.
- **RESOURCE:** Ethical Guidelines for Educational Research, British Educational Research Association (BERA). https://www.bera.ac.uk/researchers-resources/publications/ethical-guidelines-for-educational-research-2011
- **RESOURCE:** Research Ethics Training Curriculum, FHI360. https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html.
- **RESOURCE:** Conducting Mobile Surveys Responsibly, World Food Programme (WFP). http://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf.
- **RESOURCE:** The Signal Code: A Human Rights Approach to Information During a Crisis, Harvard Humanitarian Initiative. https://signalcodeorg.files.wordpress.com/2017/01/signalcode_final7.pdf
- **RESOURCE:** Research Data Security: Protecting Human Subjects' Identifiable Data, University of California, Berkeley, Human Research Protection Program. http://cphs.berkeley.edu/policies_procedures/ga106.pdf
- **RESOURCE:** Framework for Creating a Data Management Plan, ICPSR. http://www.icpsr.umich.edu/icpsrweb/content/datamanagement/dmp/framework.html
- **RESOURCE:** Data Security, University of California, Berkeley, Committee for Protection of Human Subjects. http://cphs.berkeley.edu/datasecurity.pdf