**Ethics and Responsible Data Maturity Model**

|  |
| --- |
| ***Purpose:*** *The Ethics and Responsible Data Maturity Model is intended to be a self-assessment tool applicable to different levels of the organization (whole organization, Country Office, Program or Project Team). The Model should help us become aware of our strengths and weaknesses and to develop goals for improvement. This basic Model would be supplemented with a short introduction, glossary, and simple tools/guidance on how to use it for self-assessment. Ideally an organization would be close to ‘mastering’ before placing itself in the ‘leading’ stage.* ***Contact:****lindaraftree@gmail.com* *and* *kelly.church@care.org* |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
| **Awareness and capacity** | Limited or no awareness of the need for a responsible and ethical approach to data and data-related efforts or partnerships  | Some staff and/or leadership are aware and pushing the rest of the organization to do more about data ethics and data privacy/security | Leadership and staff across the organization are aware of the need for responsible and ethical approaches to data, some have been trained, some job descriptions specifically include this area | All staff are regularly trained on Responsible Data and ethics and well-versed in the organization’s approach and policies  | Organization is a leader and ‘go-to’ authority on ethics and responsible data approachesOrganization is supporting partners, grantees and/or subcontractors to improve their privacy and security practices |
| **Policy, guidelines and practices** | No responsible data management policies or privacy promoting practices | Some groups or teams are creating their own checklists, tools, and guidelines but there is no organizational level policy or consistent procedures or practices | There is general buy-in at all levels of the organization for Responsible Data and ethics guidelines and these are being drafted with input from the wider organization | Responsible data policy and practices are in place and regularly monitored, updated, and improved, including with regard to new legislation, changing technology, or other context changes.  | Organizational policy, guidelines and practices are open source and shared with the wider sector for on-going learning and improvingLocal partner organizations are supported to develop their own data policies and guidelines as feasible |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Data partnerships** | Staff and leadership enter into partnerships that include data sharing but do not assess them in terms of their data approach and potential for harm | Staff and leadership are beginning to question how to approach data in partnerships and what due diligence aspects need to be raisedSome partnerships are assessed in terms of responsible data before agreements are made, often because of an individual or team’s concerns | Responsible data approaches are emphasized as a key element of any partnership or initiative and due diligence guidelines on data and data ethics are being developed | Staff and leadership do not enter into any type of partnership without first conducting data-related due diligence and ensuring responsible and ethical data approaches | Organization is a vocal advocate for responsible and ethical data partnerships and regularly raises this issue with its partners and the wider sector |
| **Data inventory, identification, and classification** | No understanding of what data the organization holds, where it is held, or who has access to it | Some teams or individual projects or programs keep track of the data sets they hold and restrict access to personal, sensitive or contextually-risky data by role, but this is not an organization-wide practice | An organization-wide data inventory has been conducted and personal, sensitive, or contextually risky data is documentedThere is clarity on where data is held and role-based restrictions on who can access itThere is clarity on how personal, sensitive or contextually risky data is used, by whom, and for what | A standardized data inventory process is in place across the organization in support of organization learning and knowledge managementA regular process for reviewing and adjusting role-based access to data (for both staff, external consultants, and contractors) is in place and regularly implemented across the organization | Organization supports and encourages its staff and partners to conduct data inventories and better manage secure access to data |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Data privacy rights** | There is no awareness of or concern for privacy rights or informed consent and no understanding of how to communicate them\*\*Note: Data Subject Rights* right to be informed
* right to access
* right to rectification
* right to be forgotten
* right to restrict processing
* right to data portability
* right to object to processing
* right not to be evaluated on the basis of automated processing
 | Most staff are familiar with informed consent and data privacy rights/data subject rights, but are unsure of how to manage them, especially in situations where data is digitalConsent processes are in place for certain activities, but they have not been updated or standardized, and/or they do not account for digital data and emerging digital approaches and legislation | Most staff are aware of data subject rights and working to ensure they are respected and communicated appropriately in any data initiativeAs part of organization-wide data policies, consent processes are being updated to ensure data subject rights are respected | There is consistent implementation of organization policy requiring that staff communicate with individuals, groups and communities about the personal, sensitive or potentially risky data being collected and why, with whom it is shared and for what purpose(s), any potential risks involved, how long data will be retained, their data subject rights, and who to contact with any complaints Information about data processing is consistently provided in clear and appropriate ways, considering aspects such as age, culture, literacy, data literacy, gender and contextFront- and back-end systems are capable of complying promptly with data subject requests and complaints | Data subject rights, informed consent and other privacy protective measures are consistently improved and vocally supported by the organization and its staff, and good practices are regularly shared with the wider sectorThe back-end system for responding to data subject requests and/or complaints is functioning well and seen as a model for other organizations wishing to successfully and responsibly manage data  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Legal Frameworks** | There is no awareness of privacy laws that exist in different countriesThere is no understanding of lawful bases for personal or sensitive data collection, use, and retention/ destruction | Some staff and leadership are aware that there are different legal regulations in place for different types of data collection and useThere is no consistent guidance or access to legal support when designing data collection/use plans and methods | Staff and leadership across the organization are aware that there are different legal frameworks to consider and different lawful bases for data collection according to countyThere are emerging processes to support teams to make sense of different legal frameworks and lawful bases for data collection during any data collection and use exercise | Legal review and lawful data capture and use is a part of any effort that includes data collection or use, and staff have sufficient expertise and/or support to ensure that data collection and use is legally compliant (or guidance is provided for cases where legal compliance could place data subjects and/or local organizations at extreme risk or where legal regulations are in conflict with one another)Organization privacy policies are documented, comprehensive, aligned with local legal regulations, and widely communicated in plain language to data subjects | Organization is often consulted or lauded by others for its understanding and/or application of global legal frameworks related to data |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Risk assessment and mitigation** | No context analysis or benefits-risks-harms assessment (or privacy impact assessment/ PDIA) of data collection and use plans and practices | Some teams are doing assessments to determine potential for risks and harms related to data, but this is ad hoc | Processes are being developed to support teams to assess the potential benefits, risks, and harms resulting from collection and use of personal, sensitive, and contextually risky data from vulnerable individuals or groupsBenefits-risks-harms assessment processes are participatory when possible, and always informed by local context and wider technology and data trends | There is a standard process for assessing potential benefits, risks and harms resulting any projects or programs that include sensitive, personal data, or contextually risky data that could put individuals, groups or organizations into harmEvery project or data-initiative is assessed for privacy- and data-related risks or harms during the design phase and at certain other trigger points such as context change or technology change | Privacy and data-related risks and harm assessments are consistently conducted and taken seriously in terms of go-no-go decisions on projects and partnershipsThese assessments are shared and discussed with potential partners who are encouraged to also adopt similar practices |
| **Data minimization** | Data is collected with no thought as to what it will be used for, who will use it, and whether there is capacity to use and manage it | Teams are beginning to question whether they should be collecting certain data and whether they need it or will be able to use it  | Teams are only collecting data when there is a clear and legitimate purpose and they have a plan, capacities, and budget in place for using it | Every data collection effort is required to have a clear plan for collecting a minimum amount of data with a specific and legitimate purpose | Organization has systems in place to manage and ensure data minimization is practicedOrganization advocates for data minimization externally and requires it when joining in external partnerships |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Data transmission** | No awareness of the potential risks to individuals or groups when transmitting personal or sensitive data  | Some teams are using encryption or secure file transfer tools and processes but there are no common tools or consistent practicesOfficially recommended tools and protocols are not being adopted by staff in all cases | Official file-sharing / data-sharing tools, protocols and processes are being developed to protect data privacy and securityStaff are aware of why these tools and processes are a better choice and are adopting them | Official file-sharing / data-sharing tools, protocols, and processes are mandatory for staff and partners There is widespread organizational adoption of these tools, protocols and processes | Data transmission policies, protocols, and processes are consistently monitored and improved uponPartners are widely adopting these tools, protocols and processes |
| **Data security** | No awareness of data security measures or what is in place to protect data or why it matters | Staff and leadership are aware of recommended data security policies and measures but do not regularly follow themData security measures are not adapted to local contexts, low bandwidth operating environments, or new types of digital data  | Data security policies and procedures are being updated to respond to/adapt to changes in context, laws and technologyStaff are being trained and made more aware of the need for these policiesWhere weaknesses have been detected, improved security measures have been put in place | All staff are trained on updated data security policy and proceduresThere is consistent compliance with data security policies and procedures | Data security policies are monitored and improved regularly; security tests are regularly conducted to test for weaknessesOrganization is widely known as an expert in data security in the sector |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Data sharing and open data** | No understanding or record of current data sharing or open data practices and no written data sharing agreements in place | Some staff are assessing potential risks that come with data sharing and open dataSome staff are including data sharing language in contracts and other agreementsSome staff are reviewing third-party data handling to ensure it is privacy protectiveSome staff are using de-identification techniques but this and all of the above are ad hoc, and learning is not widely shared | Staff and leadership understand how to assess data sharing and open data contractual requirements for potential risk or ethical issues and an organization-wide process for assessing benefits, risks and harms of sharing or opening data is being developedA due diligence process for assessing third party data handlers (including contractors, consultants, on-line data processors, etc.) and any other type of data sharing arrangements is being developedA standard data sharing clause is being developed by the organization’s legal counsel for use in partnership agreementsTactics for de-identification of data are being explored to reduce risks of re-identification or harm due to data sharing or open data requirements | Benefits-risks-harms assessments are consistently conducted, and their results respected and implemented with regard to any data sharing or open dataDue diligence is conducted on any third-party data handlers (including contractors, consultants, on-line data processors, etc.) or other type of data sharing arrangement before any data is shared Data sharing agreements are in place and enforced for all consultants, contracts and agreements and consistently monitored for complianceAll data that is to be shared or opened is de-identified and a risk assessment conducted to weigh benefits versus harms of sharing and opening data | Good practices are shared with the wider sector and have influenced greater care with data sharing and open data |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Data combining (mosaic effect), big data analytics, and machine learning** | No awareness of the potential risks of re-identification or other harms when data sets are combined, or big data and machine learning are used | Some staff and leadership are aware of potential risks due to new data analytics approaches, but there is nothing in place to assess or mitigate potential risks  | An initial framework and guidelines are being developed or adopted and piloted to assess potential risks of combining data sets, big data analytics, machine learning, and other emerging approachesPrivacy enhancing practices and techniques are being tested for applicability to the types of data sets in question | Before data sets are combined or big data or other emerging approaches are considered, a thorough assessment is conducted to weigh potential benefits, risks and harms to vulnerable individuals or groups Privacy enhancing techniques and practices are in place to reduce to the degree possible any re-identification of data or harm to data subjects | Organization advocates for greater care when combining data sets and using big data and other emerging approaches and has examples to share with the wider sector of good practices related to themOrganization is on the cutting edge of identifying new ways to safely use and analyze data while considering and mitigating potential harms |
| **Data retention and destruction** | No data retention or destruction plan and no awareness of why it matters | Some staff are beginning to think about and establish time periods for data retention and destruction | An initial data retention and policy is drafted and in process of testing and applicationNew initiatives are beginning to incorporate data retention and destruction plans with clear processes in place | Data retention and data management policies and procedures are established, and staff and leadership trained on them and are consistently following themData is consistently managed in ways that ease data discovery, retention and destruction Systems are in place to automate these processes where possible | Data retention policy is regularly updated to reflect applicable legal frameworksOrganization shares its data policies openly for others to learn from and adapt/apply |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AREAS** | **UNAWARE** | **AD-HOC** | **DEVELOPING** | **MASTERING** | **LEADING** |
|  |  |  |  |  |  |
| **Incident response and data breach management** | No awareness around potential risks of a data breach or the need for a data breach policy/plan | Some staff are concerned about the possibility of a data breach and seeking support to design preventive and reactive actions in case of one | A data breach policy has been drafted and is being testedRoles and responsibilities for a data breach have been established | The organization has successfully identified and prevented attempted data breaches, and/or responded to them smoothly and successfully | Data breach policy is tested annually for effectiveness and adapted to improveData breaches are openly shared with the wider sector in order to support learning and improved security overall |
| **Accountability** | No one is accountable for responsible data management | Some team members have been assigned responsibility for responsible data management, but this is ad hoc and reactive | Organization-wide responsible data policy and procedures are being developed and tested, including the chain of accountability | Organization-wide policy and procedures for responsible data are in place, and staff and leadership have been trained on themBudgets, technology, and staff are in place where needed to ensure compliance and accountability to the policy and procedures | Accountability for responsible data is clearly assigned to leadership (including the board) and embedded across the organization and all staff are clear on their roles and responsibilities with regard to data managementThe organization regularly feeds back to the sector on its responsible data efforts, including failures and improvement |
|  |  |  |  |  |  |