# **Privacy Impact Assessment (PIA) - Guidance**

**Frequently Asked Questions**

* [What is a Privacy Impact Assessment (PIA)?](#t36vmps2dc7o)
* [Is there an example PIA I can refer to?](#bs03btwrfb1r)
* [Is a PIA required for every new program, project, or technology?](#lk2474qsyxgs)
* [Can we combine multiple projects into a single PIA?](#2q1hnut5mj6o)
* [Can we refer to a previous PIA on a new program?](#m40ipp2lhoto)
* [If a new program has multiple data collection activities, with different methods, technologies and data types, is a separate PIA required for each activity?](#qr5grcurbj7)
* [Should a PIA feed into the risk register for a program?](#i83ibnldw7it)
* [If my project involves obtaining information from a data provider or third party, how can I tell if they have a legitimate interest to provide access to that data?](#om15qj8mk4mm)
* [How do I determine how long data or records should be stored or retained?](#rcj2qxb46kjx)
* [How is data de-identified?](#kg5zm3mw4cdi)
* [How do I know if a partner, subrecipient or data provider is compliant with Mercy Corps’ data privacy and data protection standards?](#jayzpv9fxqkc)
* [How do I know if we have the necessary training for staff, so that new systems are operated securely?](#60wmx31gifsp)
* [How does Mercy Corps handle data or privacy breaches?](#mnrn8hvt2qcc)

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment assists organizations in identifying and managing data privacy risks associated with any new activity, such as new programs, technology, or policies. To ensure standardization of PIAs across the agency, we have created a PIA template, an example PIA (Podio) and this guidance document.

Is there an example PIA I can refer to?

Yes. In this folder you will see one for Podio, which is a cloud-based data collaboration platform.

Is a PIA required for every new program, project, or technology?

If your program, project or technology will involve personal data, then yes. Privacy Impact Assessments assist Mercy Corps in identifying and managing data privacy risks associated with any new activity involving personal data, such as new projects, programs, technology, or policies. If your new project is extremely similar to a previous one, you may be able to save time and refer to a previous PIA.

Can we combine multiple projects into a single PIA?

It depends. As long as all the projects use the same data collection methods, technologies and data types, then yes, a single PIA is wise.

Can we refer to a previous PIA on a new program?

Absolutely -- depending on the scope of the original PIA.

* If the original PIA is identical in personal data scope and technology used, you do not need a new PIA. Your new program can simply refer to the original PIA.
* If your program uses either the same personal data or technology, your PIA can heavily reference the original. This will save a lot of time.
* If your new program will use different technologies and personal data, a brand new PIA is required.

If a new program has multiple data collection activities, with different methods, technologies and data types, is a separate PIA required for each activity?

It depends. The PIA must be easy to understand, and there is only so much room within the template. Look for ways to consolidate. Say you have five data collection activities for a program:

* If each data collection activity has its own method, technology and set of data types, then you need five PIAs.
* If two activities are extremely similar, and the other three are extremely similar, then you likely only need two PIAs -- one for the first set of two, and another for the set of three.

Should a PIA feed into the risk register for a program?

Yes. Privacy Impact Assessments help identify and manage data privacy risks associated with any new activity, such as a program. As such, they are perfect items to enter the risk register for a given program.

If my project involves obtaining information from a data provider or third party, how can I tell if they have a legitimate interest to provide access to that data?

To determine if a provider has a legitimate interest to hold and share the data being provided to Mercy Corps, confirm that informed consent was collected, and confirm or ask if a data sharing agreement (DSA) is in place.

* Informed consent gives the provider the permission to obtain and use the data.
* Legitimate interest gives the provider the right to share the data with a third party (Mercy Corps), but only if a DSA is in place.

How do I determine how long data or records should be stored or retained?

All data has a lifespan. Some data must be retained for several years, for audit purposes. Personal data from participants has a lifespan that is to be restricted to the time necessary to perform the task or need as outlined in an informed consent form. Once data has reached the end of its lifespan within the agency, it must be destroyed.   
  
To understand more about program data’s lifespan within the agency, please see Program Record Retention, or consult your program, finance or compliance manager. Other resources:

* USG-funded programs: search the [Code of Federal Regulations](https://www.govinfo.gov/help/cfr)
* Guidance on [USAID submissions to the Development Data Library](https://www.pciglobal.org/open-data-compliance/)

How is data de-identified?

De-identification of data involves removing or altering the original data, so that a particular data subject cannot be identified. Two types of de-identification are anonymization, and pseudonymization.

* Anonymization involves removing portions of the data, or otherwise generalizing ranges of data. The data is no longer considered to be PII and is no longer required to adhere to an informed consent agreement. The agency can still benefit from keeping the data for research, but it is no longer connected to the user that it came from.
* Pseudonymization de-identifies the data, often using a special key or identifier that is stored separately from the data itself. Since the special key allows the data to be re-identified, this data must continue to adhere to an informed consent agreement.

De-identification resources

* [Responsible Data Forum: Anonymising Data](https://responsibledata.io/resources/handbook/chapters/chapter-02c-sharing-data.html#anonymising-data)
* [ICO: Anonymisation: Managing data protection risk - code of practice](https://ico.org.uk/media/1061/anonymisation-code.pdf)

How do I know if a partner, subrecipient, data provider or technology is compliant with Mercy Corps’ data privacy and data protection standards?

There are a few ways to do this. One is to ask them what their current standards are, and ask them to provide documents that demonstrate their policies. Another is to provide a copy of our Responsible Data Policy, and ask if they currently abide by the policy standards in section 3.   
  
Note: if a program has subrecipients, or Mercy Corps is a subrecipient, you will need to make sure the agreement for that engagement also refers to the standards mentioned in our Responsible Data Policy.  
  
In the future, Mercy Corps will have a data sharing agreement (DSA) template, which will include a checklist for assessing data privacy and protection standards with third parties.

How do I know if we have the necessary training for staff, so that new systems are operated securely?

There are two aspects to this question: understanding the new system, and best practices for the new system. The system implementation and/or program management team is responsible for making sure that team members understand how to use the system at a basic level.

To ensure secure operation of the system, best practices must be established. This usually involves limiting the number of team members with access to the system, restricting permissions so that people only have access to what’s needed for their role, and ensuring all other security options for the system are in place. Once these best practices are established, team members must be trained accordingly.

How does Mercy Corps handle data or privacy breaches?

First, summarize the information you have, regarding a potential breach. Be sure to include the name of the system(s) impacted, type of data, and key people or teams involved. Second:

* If you only suspect a data or privacy breach, please contact [dataprotection@mercycorps.org](mailto:dataprotection@mercycorps.org)
* If you are 100% sure there has been a data breach, please contact [itsecurity@mercycorps.org](mailto:itsecurity@mercycorps.org)

For other Privacy Impact Assessment-related questions, please contact [dataprotection@mercycorps.org](mailto:dataprotection@mercycorps.org).