UAB Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a way to systematically and comprehensively analyze processing to identify and minimize data privacy and protection risks.

DPIAs should consider compliance risks and the broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or society at large, whether physical, material or non-material.

To assess the level of risk, the DPIA must consider the likelihood and the severity of any impact on individuals. The DPIA does not have to indicate that all risks have been eradicated. But it should document and assess whether or not any remaining risks are justified. Please provide your response to the questions in the Response column.

Step	Question	Response
Section 1: Identify the grant, project, or initiative goals	Explain the goals for the contract, project, or initiative and what type of data it involves. Please attach documents such as the contract, data protection or processing agreement, statement of work, etc.	
	Please specify if UAB is acting as the Controller, Co-Controller, or Processor for this contract, project, or initiative. *Definitions - Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.*	
Section 2: Describe the scope of the processing	What is the source of the data?	
	Will UAB patient data be included in the contract, project, or initiative?	

Step	Question	Response
	Please specify where the infrastructure is located that will process, store and transfer data (e.g., UAB IT, HSIS, Dept. of Medicine, Hybrid, Cloud).	
	How many individuals will have data collected about them? Please list the number of individuals by country.	
	What data elements will you be collecting and using? Please attach a Data Dictionary if available.	
	Will the data be anonymized or pseudonymized? Please explain.	
	Does the content include any of the following special categories or criminal offense data? • Personal data revealing racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Genetic data and biometric data processed for the purpose of uniquely identifying a natural person. • Data concerning health. • Data concerning a natural person's sex life or sexual orientation.	
	How long will you keep the data?	
	How frequently will data be collected?	
	Will you be using third parties to process the data?	
	Is the data encrypted in storage and transfer?	
	From what geographical area(s) is the data collected?	
Section 3: Describe the nature of the data processing	Describe the nature of the processing. *Definition - Processing covers a wide range of operations, including the collection, recording, structuring, storage, adaptation or alteration, retrieval,*	

Step	Question	Response
	consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. Please attach any flow or other diagrams as needed.	
	With whom will you be sharing data?	
Section 4: Describe the context of the processing	What is your relationship with the individuals for which data will be collected?	
	How much control will the individuals have regarding their data?	
	Would the individuals expect you to use their data in this way?	
	Do individuals include children or other vulnerable groups?	
	Are there prior concerns over this type of processing or known security flaws with the processing?	
	Is the processing of data novel in any way?	
	Are there any current issues of public concern that you should factor in?	
	Please specify if the data is covered by any privacy or security laws (HIPAA, GDPR, GLBA, FERPA, etc.)? If "Yes", please specify which ones.	
Section 5: Describe the purposes of the processing:	What do you want to achieve?	
	What is the intended effect on individuals?	
	What are the benefits of the processing?	

Step	Question	Response
Section 6: Assess necessity and proportionality	If data is being received from EEA countries, please select the lawful basis for processing from the list below. If the lawful basis is unknown, please leave it blank, and we will contact you to complete this question. (a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. (b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. (c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations). (d) **Vital interests**: the processing is necessary to protect someone's life. (e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. (f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. *For departments acting as controllers please specify one or more lawful bases. For departments that are processors please supply the lawful bases of the controller.*	
	Do you need all of the data that is collected to achieve your purpose?	
	Is there another way to achieve the same outcome?	
	How will you prevent function creep?	

Step	Question	Response
	How will you ensure data quality and data minimization?	
	What information will you give individuals?	
	How will you help to support individuals' rights?	
	If you are using third-party processors, what measures do you take to ensure processors comply?	
Step 7: Identify and assess risks and mitigations	If directed by the UAB Data Protection Officer, complete the UAB Data Protection Impact Assessment Risk Score spreadsheet.	