Data Protection Impact Assessment

Assessment Completed By:	Kristen Bosse, Sr. Director - Product Management
Signature:	DocuSigned by: Kristen Bosse Signer Name: Kristen Bosse Signing Reason: I am the author of this document Signing Time: 28-Apr-2023 | 9:22:46 AM PDT 04B7D5E3152E43FD8DEA08B87FF3B5F5

Assessment Reviewed By:	Matt Salafia, VP Engineering
Signature:	DocuSigned by: Matt Salafia Signer Name: Matt Salafia Signing Reason: I have reviewed this document Signing Time: 28-Apr-2023 | 9:25:07 AM PDT 4D054811DEA24890B79DE1EF60174989

Assessment Approved By:	Marc Wartenberger, Director, Security, Corporate QA & Compliance
Signature:	DocuSigned by: Marc Wartenberger Signer Name: Marc Wartenberger Signing Reason: I approve this document Signing Time: 29-Apr-2023 | 6:02:18 AM PDT C309572B684945489981E407C590D7F3

Assessment History	
Date	**Description**
27-Apr-2023	Initial Assessment

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
<u>Purpose specification</u> Is the data to be collected to be used only for a specified purpose?	CRIO may utilize data collected through the CRIO application for purposes beyond the contractual agreements.	The purpose of the processing of the data is contractually defined.	● Risk sufficiently mitigated

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
Will the data collected be used for anything other than the specified purpose?			
Data Limitation Is all the personal data collected necessary for the processing activities by CRIO?	Data collected beyond the scope of contract may lead to additional exposure of data in case of a data breach.	Data collection is limited to basic user information to set up a user account. For patients, the data collected through the CRIO app is limited to protocol-specific health data.	● Risk sufficiently mitigated
Right to information Are individuals explicitly informed about why their personal data is being collected and how it may be used?	Not providing individuals with clear and easily accessible information regarding their policies, procedures and practices on the collection of information may lead to a decline in trust of the application and users and patients decline to participate.	CRIO maintains a dedicated user privacy policy (**POL-004**) that describes the rights of a user. This policy is available within the CRIO application as well as CRIO's publicly-facing website.	● Risk sufficiently mitigated
Legal basis for data processing/transfer	Lack of consent or an unclear consent may lead to a complaint by a user (or	Upon enrollment, patients must sign an informed consent form. Clinical trial data collection	● Risk sufficiently mitigated

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
Consent Is consent limited to a specified purpose? If the personal data were to be used for a purpose other than that originally specified (a secondary purpose), will a new consent be sought from the individual? Alternative legal basis Is data also collected of individuals who are not present?	multiple users) to the data protection authority.	may only continue after the site has collected informed consent from the patient.	
Right to access / Rectification / Deletion Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal	Unclear instructions regarding a user's rights may lead to a complaint by a user (or multiple users) to the data protection authority.	CRIO's user privacy policy (**POL-004**) provides clear instructions regarding a data subject's rights as well as the contact information to initiate a data subject request. Upon receipt of a data subject request, CRIO has established **SOP-QMS-007 Data Subject Request** to address the	● Risk sufficiently mitigated

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
information?		request in a timely manner.	
Information quality and accuracy What processes are in place for ensuring information quality, i.e., that the information is relevant, reliable, accurate, actionable? Is there a policy or procedure in place to correct data that has already been shared with partners, or to notify partners about updates?	CRIO is unable to ensure the reliability of the information collected through the application.	CRIO application users are trained on the application - this requirement is also in place to comply with U.S. FDA 21 CFR Part 11. Further, application users participating in clinical research are also bound by Good Documentation Practices which must be adhered to. Lastly, clinical monitors are utilized in trials to review and monitor the data that has been collected.	● Risk sufficiently mitigated
Appropriate security measures What personal information is to be collected? Could disclosure of this information put the person in danger (for example information relating to ethnicity, religion, sexual orientation,	Inadequate security measures such as weak passwords, lack of employee security training may lead to a higher risk of data breaches through hacking, social engineering, phishing and other cybersecurity attacks.	All data is encrypted (256-bit AES) in transit to CRIO's databases and is maintained in pseudonymized form within CRIO's systems. CRIO employees are undergoing periodic security training.	● Risk sufficiently mitigated

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
political views, trade union membership, etc.) Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organization subject to surveillance? What preventative measures are in place? Does the processing involve external organizations or third parties? Does this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? Is information limited to others on a “need to know” basis? Is training given to all staff on		All CRIO email communications are encrypted by CRIO’s email provider. CRIO enforces a strong password rule (min 8 chars, upper, lower, special) for all users. CRIO’s integration with the Pluto Health service utilizes HTTPS for any data transmissions.	

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
good data protection and information security practices? Are emails encrypted? What kind of encryption is used? What action will be taken if there is a data breach? Are individuals informed if their personal data is lost, stolen or other compromised? Will any other organizations be informed? Have you considered some worst-case scenarios regarding what might happen if the personal data collected by your organization was compromised or deleted either by accident or purposely? How would you decide which risks are the most likely and those that are likely to have the greatest impact if the personal information were stolen,			

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
hacked, altered or stolen?			
Data sharing, disclosure/publication and/or transfer Will the personal information be shared with or disclosed to other organizations? Why? Have they provided written assurances that they will safeguard the information and not share it further? Does the organization have an adequate data protection policy?	Individuals may complain about their disclosure of their data.	Disclosure of the data to third-parties, if any, is contractually defined. CRIO utilizes Google Cloud as its infrastructure and hosting provider. CRIO periodically assesses Google's compliance against industry regulations. CRIO outlines its utilization of Google Cloud in its privacy policies which are available to the user through the CRIO app as well as the publicly-facing website.	● Risk sufficiently mitigated
Data retention Is personal information being entered into databases? Is it necessary to keep all of the data that is being	Retaining data past the contractually-defined time period can be considered a breach of contract by CRIO.	CRIO maintains all data collected for the specific time period defined within the contract with the customer. Further, CRIO must also ensure that the data retention periods allow for the data	● Risk sufficiently mitigated

Data Protection Issue	Assessment of Risks	Mitigation Measure(s)	Conclusion
processed? Are there procedures for reviewing how long data should be retained?		controller to comply with data retention periods defined by local regulators and authorities.	
<u>Accountability/Oversight mechanism:</u> Are data protection standards and procedures effectively implemented? Are oversight mechanisms in place to overview existing practices and to provide guidance to CRIO?	Lack of independent oversight and leadership may lead to inadequate controls in place to protect the data.	CRIO has installed the Director of Security, Corporate QA & Compliance as the Data Protection Officer with the specific responsibility for ensuring that CRIO's policies and procedures meet the data protection expectations.	● Risk sufficiently mitigated

Impact Assessment Summary	
Assessed Risk	High

The nature of the data processed means that any system will always have a high risk to the security and privacy of that data. CRIO has implemented a number of mitigation controls to help reduce this risk, but they do not eliminate it entirely. CRIO Engineering, Product Management, and Corporate QA & Compliance will continue to monitor CRIO's security practices on a regular basis and make adjustments to its mitigation controls as needed.