US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/27/2026

OPDIV:

NIH

Name:

NIAID CRIMSON LabKey

PIA Unique Identifier:

P-1699425-496704

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

Clinical Research Information Management System of the National Institute of Allergy and Infectious Diseases (NIAID) (CRIMSON) LabKey is used as a study portal containing study artifacts and operational status reports. It is used in the collection and management of study source documents, case report forms (CRFs), and the data associated with the CRFs. It is also used for sample tracking. The system interfaces with several Clinical Data Management Systems (CRIMSON Research Electronic Data Capture (REDCap), DFdiscover), as well as several reporting and visualization tools, such as R, which is a programming language.

CRIMSON LabKey supports study administration, data management operations, study coordinators, study monitors/auditors, as well as study safety, pharmacy, and laboratory teams, in various locations both domestic and international.

Describe the type of information the system will collect, maintain (store), or share.

For study management, CRIMSON LabKey contains CRF information associated with a study, which

includes a de-identified study/patient identifier (ID), as well as study data such as vital signs, demographics, medications, adverse events, and laboratory results. None of this data is personally identifiable information (PII). This information comes from CRIMSON REDCap. Users can also upload study-related documents and are not supposed to upload anything containing PII. If PII is discovered, the data management team would review it and remove it.

For sample management, CRIMSON LabKey collects the following non-PII: study ID, sample ID, sample type, and sample location. Users provide the following PII for account provisioning and for communications: name and email address. Users can edit their own profile and add a phone number.

The source system for PII used for provisioning accounts (name, email address) for CRIMSON LabKey NIH users comes from the NIH Enterprise Directory (NED). NED maintains its own privacy impact assessment (PIA), including all legal authorities documented.

NIH users log into this system using the NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own approved PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service that facilitates and governs network access to various resources.

For non-NIH users, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user's login credentials. NIH Federated login enables users to use a single authentication method via an individual's parent organization. After the system owner approves access to an individual and registers their parent organization's identity provider, individuals are redirected to their parent organization's identity provider for credentials. NIH Federation Services resides within the NIH IAM Services, and maintains its own PIA, including all legal authorities documented.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

CRIMSON LabKey is used as a study portal containing study artifacts and operational status reports. It is used in the collection and management of study source documents, CRFs, and the data associated with the CRFs. It is also used for sample tracking. The system interfaces with several Clinical Data Management Systems (CRIMSON REDCap, DFdiscover), as well as several reporting and visualization tools, such as R.
CRIMSON LabKey supports study administration, data management operations, study coordinators, study monitors/auditors, as well as study safety, pharmacy, and laboratory teams, in various locations both domestic and international.

For study management, CRIMSON LabKey contains CRF information associated with a study, which includes a de-identified study/patient ID, as well as study data such as vital signs, demographics, medications, adverse events, and laboratory results. None of this data is PII. This information comes from CRIMSON REDCap.

Users can also upload study-related documents and are not supposed to upload anything containing PII. If PII is discovered, the data management team would review it and remove it.

For sample management, CRIMSON LabKey collects the following non-PII: study ID, sample ID, sample type, and sample location.

Users provide the following PII for account provisioning and for communications: name and email address. Users can edit their own profile and add a phone number.

The source system for PII used for provisioning accounts (name, email address) for CRIMSON LabKey NIH users comes from NED. NED maintains its own PIA, including all legal authorities documented.

NIH users log into this system using the NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own approved PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service that facilitates and governs network access to various resources.

For non-NIH users, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user's login credentials. NIH Federated login enables users to use a single authentication method via an individual's parent organization. After the system owner approves access to an individual and registers their parent organization's identity provider, individuals are redirected to their parent organization's identity provider for credentials. NIH Federation Services resides within the NIH IAM Services, and maintains its own PIA, including all legal authorities documented.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Phone Numbers
Demographics

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

PII (name, email address) is only used for provisioning user accounts and for communications with users.

Describe the secondary uses for which the PII will be used.

PII can be used by CRIMSON LabKey developers when testing the application.

Identify legal authorities governing information use and disclosure specific to the system and program.

45 CFR 46; 42 USC 241; 42 USC 282; 42 USC 284; 42 USC 285f

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0216 Administration: NIH Electronic Directory

09-90-0777, Facility and Resource Access Control Records

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

Not applicable. Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act requirements.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The PII collected and used for provisioning NIH CRIMSON LabKey user accounts (name, email address) comes from NED. NED maintains its own PIA, outlining the process to notify individuals that their PII is collected.

Non-NIH CRIMSON LabKey users provide contact information such as name and e-mail address, which is used for provisioning accounts and communications, and understand that the contact information is not used for any other purpose other than for provisioning their account and for communications with the user.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no op-out for NIH CRIMSON LabKey users, as the collected PII used for provisioning accounts (name, email address) is from NED. NED collects the PII during the hiring process. An individual may decline to give their PII, but that would remove them from the hiring process. NED maintains its own PIA.

There is no opt-out for non-NIH CRIMSON LabKey users as the collected PII (name, email address) is needed for provisioning their account and communications with the user.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

CRIMSON LabKey users provide contact information (name, e-mail address) for provisioning their accounts and understand that the contact information is not used for any other purpose other than communications with the user. A notification and consent process is not required at this time as the contact information is not expected to be used for anything other than user notification.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

CRIMSON LabKey users provide contact information (name, e-mail address) that is used for communications with the user. Users who need to correct their contact information can update their name themselves within CRIMSON LabKey. If a user needs to update their e-mail address, or if they believe their PII has been inappropriately obtained, used, or disclosed, they can contact

NIAIDSTORMSupport@mail.nih.gov.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

CRIMSON LabKey users are responsible for keeping their contact information current. CRIMSON LabKey administrators review accounts annually.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

System access to CRIMSON LabKey is granted for purposes of conducting clinical research. Researchers are granted access based on a "least permissions" model appropriate to their role in the research process. End users have access to their user profiles, which may include their own e-mail address and/or
phone number. Administrators have access to all PII in the system.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

For CRIMSON LabKey users, an NIH IAM Services login is required to gain access to the stored data. Non-NIH CRIMSON LabKey users use NIH IAM Services with Federation.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials. Administrators and Privileged users require additional training specific to their roles and responsibilities.

Describe training system users receive (above and beyond general security and privacy awareness training).

Additional role-based training is required for individuals with significant security responsibilities.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Patient records pertaining to CRIMSON LabKey are retained and disposed of under the authority of the following NIH Records Schedule:
Item 01-003, Records of All Other Intramural Research Projects.
Description: These records do not meet the retention criteria for Item I-0001 - Records of Intramural Research Records Projects of Historical Significance, or Item I-0002 - Research
Records that Support Intellectual Property Rights. Intramural research records related to planning,

development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs).
Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff. Disposition Authority: Disposition Authority Agency (DAA)-0443-2012-0007-0003

Login /Systems Access Records are retained and disposed of under the authority of the following NIH Records Schedule:
Item 07-203, System Access Records. Systems not requiring special accountability for access. Description: These records are created as part of the user identification and authorization process to gain access to systems. Systems not requiring special accountability for access. These are user identification records generated. Disposition: Destroy when business use ceases. Disposition Authority: DAA-GRS-2013-0006-0003

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: The system had a security assessment and authorization (SA&A) performed in accordance with NIH and HHS requirements. SA&A documentation including the following were developed as required: security categorization, e-authentication risk assessment, system security plan,
evidence of security control testing, and plan of action and milestones. Applicable Privacy Act clauses are inserted in solicitations and contracts as applicable. Policies for the retention and destruction of PII are in place. Backups of system data are performed on a regular basis.
Technical Controls: User authentication services are provided by the NIH IAM Services (with Federation). Roles in CRIMSON LabKey are used to control who has access to PII. End users have access to their user profiles, which may include their own e-mail address and/or phone number. Administrators have access to all PII in the system. Data travels only over secured NIH networks. Intrusion detection is provided by the NIH network at the perimeter and other points within the network. The NIH Incident Response Team is responsible for incident handling, response, and reporting, and will notify the NIAID Information Systems Security Officer of any incidents that may be related to the system. The CRIMSON LabKey application (Web) server is hosted in the NIH DMZ (demilitarized zone), with a backend database server inside the NIH network perimeter.

Physical Controls: System components are in NIH data centers, which have appropriate physical controls to restrict access to servers. Access to data centers is controlled by NIH Personal Identity Verification card. Visitors are always escorted.

Identify the publicly-available URL:

https://crimsonlabkey.cc.nih.gov/labkey/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null