US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/30/2025

OPDIV:

NIH

Name:

NIAID Clinical Quality Management System (NCQMS)

PIA Unique Identifier:

P-4447110-323589

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

The National Institute of Allergy and Infectious Diseases (NIAID) Clinical Quality Management System (NCQMS) is a minor application that supports the implementation of an Electronic Quality Management System (eQMS) for NIAID. This system ensures compliance with the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use (ICH) Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2) and other applicable and current clinical research regulations and requirements. NCQMS provides a unified approach to support common functionality, infrastructure, and operational support.

NIAID sponsors numerous domestic and international clinical trials. NCQMS manages quality throughout the design, conduct, recording, evaluation, reporting, and archiving of clinical trials. NCQMS follows a risk-based approach to quality management, focusing on critical processes and data identification, risk identification, risk evaluation, risk control, risk communication, risk review, and risk reporting. NIAID defines an eQMS as a web-based system for electronically logging, managing, and trending quality processes in accordance with Good x Practice (GxP) quality

standards, including 21 Code of Federal Regulations (CFR) Part 11 requirements. An eQMS must be validated for its intended purpose, which is to support trial data submissions to regulatory authorities for licensure of the investigational product.

As of October 2024, the STRIDES-based CQMS system has been migrated to the MasterControl-owned and managed FedRAMP QX instance, which is maintained via Amazon Web Services (AWS)'s FedRAMP Gov. Cloud environment.

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

NCQMS collects and stores the username/passwords, individual names, email addresses, and physical mailing addresses of NIAID staff which are contained in Lab certification details, Statement of Investigation Food and Drug Administration (FDA) form 1572, and Curriculum Vitae (CVs), which may contain the user's educational records and/or certificates. These documents are stored for operational use during the coordination of clinical trial activities.

Users log in to the various supported systems using the National Institutes of Health (NIH) Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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 user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

NCQMS collects and stores the username/passwords, individual names, email addresses, and physical mailing addresses of NIAID staff which are contained in Lab certification details, Statement of Investigation Food and Drug Administration (FDA) form 1572, and Curriculum Vitae (CVs), which may contain the user's educational records and/or certificates. These documents are stored for operational use during the coordination of clinical trial activities.

Users log in to the various supported systems using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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 user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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
Mailing Address
Certificates
Education Records
Username/password

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

Employees

Public Citizens

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

The personally identifiable information (PII) is incidental. It is not collected by the system. Rather, the system's stored documents and reports often bear the names of the staff who prepared those documents, reports, filings, etc.

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

There are no secondary uses articulated by the system operators.

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

42 U.S.C. 241, 289a

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

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.

All NIAID staff are notified that their personal information will be collected at the time of hiring.

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.

Each individual is informed of information collection practices upon orientation. Staff may not opt-out of the information collection as it is a condition of employment and used for various valid business purposes by the hospital including preparation of various documents, reports, filings, etc.

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

Business Owners and System Owners are the owners of the data within and they are responsible for

all communications that would notify the users of any changes to the system and the data therein.

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.

A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The NIH Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with the NIAID Information Systems Security Officer (ISSO) and NIH Privacy Officer.

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

PII housed within the NCQMS are validated for accuracy prior to be uploaded into the system. Those forms are then retained as part of a historical repository to track the documentation uploaded at a point-in-time and will not be changed post-upload in order to retain the historical entries within the system.

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.

Access to PII information housed within NCQMS is role based, with users being provisioned with the role with the minimum access assigned based on their job responsibilities. Access is provisioned as requested in the access request email.

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.

The NCQMS instance is configured with defined roles that control the level of permission a user is configured to have. General users are configured to only those roles that will allow the user to access only the PII necessary to perform their assigned job responsibility. If the user does not have the role(s) needed to access parts of the system where PII is located, the system will not show them that it exists.

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).

All users receive general security and privacy awareness training that is mandatory and recorded, however each Program Manager is responsible for training their users in the system's use beyond basic training requirements.

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.

The only PII housed within NCQMS application are the user’s first/last names, their usernames and

email addresses, which are deemed necessary for audit logging / investigatory purposes. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.

Includes records such as:
• user profiles
• log-in files
• audit trail files and extracts
• system usage files
• cost-back files used to assess charges for system use
Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

[Disposition Authority: DAA-GRS-2013-0006-0004]
Medical Staff Credentialing Records, participant records are temporary records that can be destroyed 30 years after cutoff, which is one year after the medical staff member leaves patient care. [Disposition Authority: DAA-0443-2012-0007-0011]

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

Administrative Controls: NCQMS has documented processes in place to determine and grant the appropriate role-based access to all data, including PII housed within the system. This access will be reviewed periodically as defined in process documentation to validate the continued access to the system and the PII.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. Access to the FedRAMP AWS Cloud's infrastructure is maintained only by the MasterControl vendor's personnel with the appropriate role/permissions needed to access it and is inaccessible to non-MasterControl vendor personnel.

Physical Controls: The infrastructure is housed within an AWS-controlled datacenter that is operated in partnership with the MasterControl vendor and is configured as required to maintain FedRAMP requirements. Only those personnel needed to have access to the datacenter are allowed to gain access. The datacenter is not accessible to NIH-users.

Identify the publicly-available URL:

https://niaid.mastercontrolgov.com/niaid

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?

Yes

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

Yes