

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/01/2024

OPDIV:

NIH

Name:

NIAID Web Content Management Solutions

PIA Unique Identifier:

P-9981886-138927

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?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

Significant System Management Change

Alteration in Character of Data

Other...

Describe in further detail any changes to the system that have occurred since the last PIA.

Control baseline from Low to Moderate. Addition of PII to the system.

Describe the purpose of the system.

The National Institute of Allergy and Infectious Diseases (NIAID) Web Content Management Solutions (NWCMS) System is a minor stand-alone application that is housed in a virtual system that is hosted within the NIAID Monarch environment. The purpose of the NIAID Web Content Management Solutions is to enable interested parties to view summary information on current NIAID activities.

NWCMS contains the sub-environments Inside Version Next (IVN/Inside) and the Human

Immunodeficiency Virus (HIV) Vaccine Research Portal (VRP), which both contain its own separate database of information and do not communicate with each other. Both environments run on the Drupal application, which is an open-source Content Management System (CMS) that hosts files and web pages in an organizational system that allows for easy updating and viewing. Both production environments are located outside the NIH firewall and are maintained by New Media Group. Changes to the Drupal application's functionality are completed through the New Media Group's promotion of code changes in the Operations and Engineering Branch (OEB)-managed GitHub repository. Business Process and Information Management Branch (BPIMB) provides additional support to the New Media Group upon their request.

IVN/Inside is used to get news out across the NIAID community and carries over a directory of NIH personnel that has been imported from the NIH Enterprise Directory (NED). The mission of the HIV Vaccine Research Portal (VRP) is to develop a safe and effective HIV Vaccine by advancing research to discover and manufacture novel vaccine candidates and by assessing correlation of immunogenicity and protection. The VRP is currently undergoing an exploratory review for potential decommissioning. BPIMB has placed a maintenance notification on its homepage to register the number of site visits between now and early 2024.

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

NWCMS contains the sub-environments Inside Version Next (IVN/Inside) and the HIV Vaccine Research Portal (VRP). IVN/Inside serves as an intranet for 4,000 NIAID and NIH users to provide up-to-date content needed to perform their daily tasks. This intranet contains a searchable directory carried over from the NIH Enterprise Directory (NED) to provide users with information on personnel and read the latest news. NIH Enterprise Directory (NED) maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented.

Information carried over from NIH Enterprise Directory (NED) include the following: first/last name, username, business mailing address, email address, phone number, and, if the profile contains one, the user's photographic identifier.

The system can also provide users with a general summary description and metrics on the current state of each solution.

The system has the capability to collect and maintain unique username and passwords for non-NIH users.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and authorize for NIH 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 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.

The National Institute of Allergy and Infectious Diseases (NIAID) Web Content Management Solutions (NWCMS) System is a minor stand-alone application that is housed in a virtual system that is hosted within the NIAID Monarch environment. The purpose of the NIAID Web Content Management Solutions is to enable interested parties to view summary information on current NIAID activities.

NWCMS contains the sub-environments Inside Version Next (IVN/Inside) and the Human Immunodeficiency Virus (HIV) Vaccine Research Portal (VRP), which both contain its own separate

database of information and do not communicate with each other. Both environments run on the Drupal application, which is an open-source Content Management System (CMS) that hosts files and web pages in an organizational system that allows for easy updating and viewing. Both production environments are located outside the NIH firewall and are maintained by New Media Group. Changes to the Drupal application's functionality are completed through the New Media Group's promotion of code changes in the Operations and Engineering Branch (OEB)-managed GitHub repository. Business Process and Information Management Branch (BPIMB) provides additional support to the New Media Group upon their request.

IVN/Inside is used to get news out across the NIAID community and carries over a directory of NIH personnel that has been imported from the NIH Enterprise Directory (NED). The mission of the HIV Vaccine Research Portal (VRP) is to develop a safe and effective HIV Vaccine by advancing research to discover and manufacture novel vaccine candidates and by assessing correlation of immunogenicity and protection. The VRP is currently undergoing an exploratory review for potential decommissioning. BPIMB has placed a maintenance notification on its homepage to register the number of site visits between now and early 2024.

NWCMS contains the sub-environments Inside Version Next (IVN/Inside) and the HIV Vaccine Research Portal (VRP). IVN/Inside serves as an intranet for 4,000 NIAID and NIH users to provide up-to-date content needed to perform their daily tasks. This intranet contains a searchable directory carried over from the NIH Enterprise Directory (NED) to provide users with information on personnel and read the latest news. NIH Enterprise Directory (NED) maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented.

Information carried over from NIH Enterprise Directory (NED) include the following: first/last name, username, business mailing address, email address, phone number, and, if the profile contains one, the user's photographic identifier.

The system can also provide users with a general summary description and metrics on the current state of each solution.

The system has the capability to collect and maintain unique username and passwords for non-NIH users.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services is to authenticate and authorize for NIH 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 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

Photographic Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Username/Passwords

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

For directory purposes.

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

Not Applicable.

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

5 U.S.C. 552a(e)(4) and (11)

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

09-90-1901 HHS Correspondence, Comment, Customer Service, and Contact List Records

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable.

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 PII information within NWCMS is imported from NED, which collects the information from employees and contractors as part of their on-boarding processes. The information is not collected through the NWCMS system itself.

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.

All PII information within NWCMS is imported from NED, which collects the information from employees and contractors as part of their on-boarding processes. The only way a user could opt-out of providing their information would be to not complete the on-boarding process with NIH.

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

All PII information within NWCMS is imported from NED, which collects the information from

employees and contractors as part of their on-boarding processes. Any notifications related to the changes within the NED system are conducted outside of NWCMS through other processes.

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.

As NWCMS contains PII pulled directly from NED, users must reach out to the NED system team to resolve the concerns, resulting in NED being updated. The NWCMS system has been configured to automatically pull the updated changes into NWCMS nightly.

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

As NWCMS contains PII pulled directly from NED, which is reviewed regularly to ensure the latest information is provided. The NWCMS system has been configured to automatically pull any updates into NWCMS nightly.

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.

End users are granted read-only access to the system in order to retrieve the directory information they are searching for with the NWCMS Inside application. Administrators require full access to the system in order to perform their daily tasks of maintaining the system. Developers are granted partial access to the system, and its databases based on the role they are assigned when on-boarded. Contractors must have their access to NIH systems granted by an NIH federal employee. Once granted, they are provisioned with the role that has the least amount of privileged necessary to complete their tasks.

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.

All user access is based on the concept of least privilege. Least privilege means that users are provided access to only the lowest level of permissions needed to conduct their daily tasks.

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. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the <http://irtsectraining.nih.gov> site with valid NIH credentials.

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

When a user is given authorization to the NWCMS system, the business owner ensures that each user is trained in its use, including access controls and restrictions.

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.

System access records are contained for 90 days within the NWCMS application. Afterwards, they are removed from NWCMS for long term storage.

NWCMS' Login Information pulled from NIH's IAM Services: Login/Systems Access Records are retained and disposed of under the authority of the (NIH General Records Schedule, Section -7-204 Information Systems Security Records.) These are temporary records. 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]

Data within the NWCMS pertains to NIH institute news and related information. This falls under the (NIH General Records Schedule for Transitory Records, Section 10-103). These are required only for a short time (generally less than 180 days) and that are not required to meet legal or fiscal obligations; or to initiate, sustain, evaluate or provide evidence of decision-making. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule.

[Disposition Authority:DAA-GRS-2017-0003-0001]

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

Each user account within NWCMS is configured to utilize access control limitations assigned to them through administrative controls. The control is the formal process of provisioning and granting role-based access rights to each portion of the system for each potential user. Role assignments are based on the Community, Information and Security (CIS) Model, which formally delineates the type of access permissions a user is given based on the role/group name. The role must be requested and approved by the Business Owner before the user will be able to see the information within the system. If a user does not have the role assignment necessary to access the information within, the user will not be able to see that it exists. Lastly, additional security training is required for all administrators with access to PII. This training is targeted explicitly for the proper security requirements for safeguarding PII.

Technical controls safeguards include restricting access to authenticated users via Federal information Process Standard (FIPS) Publication 140-2 secure socket layer encryption for all data and documents at rest. Two-factor authentication via NIH PIV card is required to log in to the system. The role-based access controls defined in the Administrative Controls are programmed into the system to secure PII data from view/access. Each administrator's access (i.e., Server administrator, Database Administrator (DBA), operating system administrator) is limited through role-based access to only those repositories where their expertise is required.

Physical controls are built into the NWCMS through automated enforcement mechanisms within the system's Monarch cloud environment. These mechanisms are provided and supported by the NIAID Office of Cyber Infrastructure and Computational Biology (OCICB) Operations and Engineering Branch (OEB). This branch is responsible for management of the servers, storage, databases, networks and operating systems used or accessed by NWCMS.

