# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

08/02/2016

### OPDIV:

FDA

### Name:

Shiny Server

**PIA Unique Identifier:**

P-2492542-217025

**The subject of this PIA is which of the following?**

Minor Application (stand-alone)

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Implementation

**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?**

New

**Does the system have Security Authorization (SA)?**

No

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

**Describe the purpose of the system.**

Shiny Server provides a mission essential capability for developing and sharing food safety risk assessment models (web apps) with a community of scientific users (FDA and non-FDA) via Internet and the FDA Intranet. It is being used to support research into various environmental risk factors associated with the potential for development, growth, mutagenesis and migration of specific food-borne pathogens of interest.

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

This system supports the development of statistical risk assessment models using a common modeling language (R-code) and data compiled from open source scientific literature.  It does not collect, store or share any information about people; it is only a web-server-based mathematical modeling tool supporting scientific risk assessments.  Access to the published web apps on the system will be controlled by implementing the authentication functionality available in the software product.

The authentication will be through authorized user accounts that will be maintained in the system. As part of the access process, scientific users (FDA and non-FDA), direct contractors, and/or FDA employees are presented with a dialog box where they enter username and a password (created by the individual user). Scientific users include FDA personnel and non-FDA persons who work for other public sector entities. When the user credentials have been authenticated, users are granted access to the published web apps that the particular user is authorized to access.

Secure sockets layer (SSL) technology is employed; transmitted information, including usernames and passwords, is encrypted.

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

Shiny Server Pro is a commercial web server software package provided by RStudio. The system consists of the Shiny Server Pro software and a suitable Linux-based server environment to host this commercial software application. Users access published web apps (risk assessment models) to perform scenario-based risk assessments. The web apps require data input from the user to define the risk assessment parameters of a given scenario.

Food safety is the focus of the scenario-based risk assessments performed. Shiny Server Pro is being used to support research into various environmental risk factors associated with the potential for development, growth, mutagenesis and migration of specific food-borne pathogens of interest. For a given defined scenario, assorted risk factors have been identified along with the relative importance of each in terms of evaluating the overall risk associated with the potential for development, growth, mutagenesis and migration of specific food-borne pathogens. Some environmental factors contribute to increased risk more than others. Understanding the relative importance of such risk factors and the specifically associated environmental conditions is one of the research objectives of the risk assessments being performed.

This data will be used to produce unique results and the user may include those results in subsequent analyses, publications and/or reference files/documents. The data does not correlate to any individual or group of individuals as it is specific to food-borne pathogens and not linked in any way to individuals. It is scientific data/information needed to characterize the environment or scenario that is being evaluated with regard to risk factors associated with the potential for development, growth, mutagenesis and migration of specific food-borne pathogens of interest.

All user entered data/information is transient and is purged when the user terminates a session. The system also stores a flat-file that contains the username and password for all authorized users and the level of access associated with those credentials. The flat-file is self-contained and not integrated into any Enterprise authentication mechanism or user/password database system. That information is maintained in the system until access to the published web apps a user or group of users is authorized to use is no longer needed. Access to the flat-file containing this information is strictly limited to the Shiny Server administrator who is an FDA employee (a single individual) and authorized direct contractors at the Ashburn Data Center.

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

Yes

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

Logon credentials only (username, password and level of access)

**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

**For what primary purpose is the PII used?**

The only PII in the system is usernames, passwords and level of access authorized for system users. This information is used for a single purpose of controlling and authenticating access.

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

None.

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

The implementation of this system is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures of the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

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

No

**Identify the sources of PII in the system.**

Email

**Government Sources**

Within OpDiv

State/Local/Tribal

Foreign

**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 user accounts are created and managed by an FDA employee who is the Shiny Server administrator. That FDA employee will communicate directly with each user and provide notice that their personal information will be collected (account credentials) in order to create a user account that is required for access to any of the published risk assessment models.

**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.**

Submission of PII is voluntary as that term is used by the Privacy Act. However, the submission of PII is necessary in order for users to access and use the system.

Scientific users (FDA and non-FDA), direct contractors, and FDA employees will provide the system with PII relevant to their access credentials. There is no method for employees to opt not to submit PII.  Users must provide their PII in order authorize and authenticate their access to specific published web apps.

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

No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the web site, or e-mail notice to the individuals.

**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.**

Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to request to rectify the situation. Often, these individuals contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. The FDA then considers these requests and, if appropriate, makes the requested changes.

Employees with such concerns can additionally work with their supervisors, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels.

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

Scientific users (FDA and non-FDA), direct contractors, and FDA employees are responsible for providing accurate information and may independently update and correct their information at any time through the Shiny Server administrator, an FDA employee.

The Ashburn Data Center has back-up servers to ensure information is readily available, even if a main server fails. Users receive an annual e-mailrequesting that they review their information and ensure that it is accurate and up-to-date. To ensure relevancy, if users provide any updates, system administrators change the individuals’ information accordingly.  Data integrity is maintained through user access recertification and encryption for data at rest and in transit.

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

**Users:**

Users will not have access to others' logon credentials.

**Administrators:**

Administrators (authorized FDA employees) may be application administrators who require access to  create and manage user accounts, but will not have access to users' self-created passwords.

**Contractors:**

Authorized direct contractors at the Ashburn Data Center may have limited access to usernames in the course of providing technical assistance.

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

The only PII in the system consists of the user access credentials. Management uses role based criteria to determine access to this information at the individual level.  Users have access only to their own username and password. Administrators may have access to usernames as necessary in the course of creating and maintaining accounts in their administrator role, they will not have access to passwords. Data center support staff who are direct contractor employees may require access as part of their technical assistance duties.

**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.**

Management establishes roles for individual personnel, with role-based restrictions employed technically to permit access only to information that is required for each individual to perform his/her job.

**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.**

The FDA requires all Agency personnel and direct contractors to complete FDA's IT Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII.

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

Additional on-the-job or informal training may be received.

**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.**

FDA File Code 9962 (GRS 20, Item 1c; superseded by the new GRS 3.2, Item 030, Disposition Authority DAA-GRS-2013-0006-0003). Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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

Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include usernames, passwords, use of SSL and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology’s (NIST’s) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.