Privacy Impact Assessment (PIA): FDA - EMS - QTR2 - 2024 - FDA2128040

Created Date: 4/9/2024 4:03 PM Last Updated: 4/30/2024 10:02 AM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	FDA - EMS - QTR2 - 2024 - FDA2128040	**PIA ID:**	1801561
Name of Component:	FDA - OC Event Management System	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	21
Submission Status:	Submitted	**Submit Date:**	4/11/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:	Low	**OpDiv PIA ID:**	FDA2128040
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	7/11/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to this system since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	Event Management System (EMS) is a user-friendly room scheduling software designed to track reservations and the details associated with them. EMS provides a wide variety of tools and utilities for creating, managing, and reporting on events. As of today, five modules of EMS have been installed and operational: EMS Workplace Client, EMS Web App, and Email Notification Services. EMS Workplace Client is used by Office of the Commissioner (OC) employees to manage reservations. EMS Web App is used FDA-wide through a link of "White Oak Conference Rooms" on FDA intranet. The Email Notification Services module provides users the ability to create group email notifications for certain events occurring in the system. Also, the Plan-A-Meeting (PAM) module and Floor Plan module. EMS 221.2.1 is in operation as of now, and an upgrade to EMS 222.2.0 is in process. The entire user community is internal to FDA. FDA White Oak and Center for Tobacco Products (CTP) at 9200 Corporate are active buildings in the system and use EMS to schedule their conference space. There are also countless FDA employees who access the system from other FDA buildings off campus and from home via the link "White Oak Conference Rooms" on FDA intranet.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The types of information that is collected, maintained, and shared are: Name, Email Address, Phone Numbers, Title of Meeting, how many participants will be a part of the meeting, Building Number, and Meeting Room Number. There is no deletion of data from our system at this time because a user is connected to reservations, they are not deleted from the system if they leave FDA. A user will become inactive and will not be able to access the system if they leave the agency, but their historical information (past reservations) will remain for reporting purposes. If a user never made a reservation, they are removed from the system.
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	EMS has three components: EMS Workplace Client, Virtual EMS Client (VEMS), and Email Notification Services. Employees of the FDA's Office of the Commissioner (OC) use EMS Workplace Client to manage reservations. VEMS is used FDA-wide through a link on the FDA intranet site for scheduling reservations. The Email Notification Services module provides users the ability to create group email notifications for certain events managed in the system. No data is shared with another system.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Every FDA employee and/or direct contractor with a valid Personal Identity Verification (PIV) has access to EMS from the EASE system. EMS is only available via Single sign-on (SSO) within the FDA intranet (not external, nor can a valid FDA user access EMS without FDA Government Furnished Equipment (GFE) and FDA PIV.
PTA - 10:	Does the website have a posted privacy notice?	No
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not Collect PII
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	

PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Other - Free text Field - email address and phone numbers are work email and work phone for FDA personnel and direct contractors.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	To contact the employee with details regarding their conference room reservations.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	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.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	

PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	An OMB collection approval number is not required because no external data is collected.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	Individuals cannot opt-out if they require use of the CCS system. Their work contact information is needed to manage room reservations.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	If the agency makes a major change in its collection or use of PII in CDER Regulatory Review (RR), FDA will notify affected individuals in the most efficient and effective manner available and appropriate, which may include a formal process involving written or electronic notice, or informal processes such as e-mail.

PIA - 15:	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. If no process exists, explain why not.	Data in the CCS system is supplied by FDA's internal EASE system and personnel may access their EASE data on their own to update or correct their information. Personnel may also contact FDA's Employee Resources and Information Center (ERIC) to correct inaccurate or out of date information. If the employee believes that his/her PII was inappropriately used or disclosed, the individual may contact the EMS Reservation Team through a dedicated email address or report it to FDA's Systems Management Center (SMC). Additionally, when an employee submits a request for a reservation through EMS, certain fields are pre-populated and visible to the employee. The employee may edit these pre-populated fields, i.e., work phone number and work e-mail address.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	To ensure integrity and accuracy CCS staff randomly check EMS web accounts to spot potential problems and constantly monitor FWI and EMS to check for bugs. Personnel may update their information within their EASE account to ensure relevancy and may also correct data fields when using EMS. The data in EASE that is transmitted from the U.S. Department of Health and Human Services (HHS) Human Resources system to ensure availability and is also subject to HHS data integrity measures.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Users for the EMS module include technicians, gatekeepers, and conference managers who have access to manage conference rooms, assign web templates, troubleshoot issues. Access to the FWI module is restricted to the FWI team which consists of administrators, there are no system users. Administrators: Administrators manage conference rooms, assign web templates, troubleshoot issues, add buildings and rooms, add resource categories, change parameters. Contractors: Direct Contractors include technicians, gatekeepers, and conference managers who have access to manage conference rooms, assign web templates, troubleshoot issues.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	For access to the EMS Client, relevant office management contacts ensure users are assigned to a user group with appropriate access limitations for their own office. To access the Virtual EMS on the FDA intranet, any user connected to the FDA network can open the virtual client through integrated windows authentication. Access to the FWI module is restricted to the FWI team which consists of administrators, there are no system users.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	System access minimization is achieved via tiered access permissions ranging from system administrator privileges to simple reporting usage. For example, direct contract personnel typically have access permitting them to reserve conference rooms and manage meetings but cannot change employee information.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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 to complete information security and privacy awareness training at least once every 12 months. A portion of this training is dedicated to the protection of PII.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All users receive training from the system owner and can obtain training via a web module if they wish. For additional privacy guidance, personnel may contact the agency's privacy office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Records are retained and destroyed in accordance with existing applicable federal retention schedules. GRS 5.1, item 010 (DAA-GRS-2016-0016-0001) -Office Administrative Files: Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists. Destroy when two years old. (N1-GRS-98-2 item 43)
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	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 uses of firewalls; access controls such as usernames and passwords; and regular testing of information technology systems. 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.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/11/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Addressed HHS comment regarding PIA-23.	**SOP Review Date:**	4/11/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	4/11/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 4/11/2024 This PIA is ready for SAOP review and approval as all comments have been addressed. PIA-23: GRS 23 is superseded by GRS 5.1, item 010 (DAA-GRS-2016-0016-0001} please update accordingly.	**Agency Privacy Analyst Days Open:**	0

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	4/30/2024
		SAOP Days Open:	19

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
OC Event Management System_SOP Approved 4.11.2024.pdf	171326	.pdf	4/11/2024 5:22 PM	0
OC Event Management System_SOP approved_PIA.pdf	168781	.pdf	4/10/2024 9:33 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 23	BLAND, CRYSTAL	4/11/2024	GRS 23 is superseded by GRS 5.1, item 010 (DAA-GRS-2016-0016-0001} please update accordingly.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	4/30/2024 10:02 AM	**History Log:**	View History Log