

Date Signed: 7/13/2022

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

Status:	Approved	PIA ID:	1460097
PIA Name:	FDA - FEAEMAIP - MuleSoft - QTR3 - 2022 - FDA2061387	Title:	FDA - OC GSS1 Network and Telecom
OpDiv:	FDA		

PTA

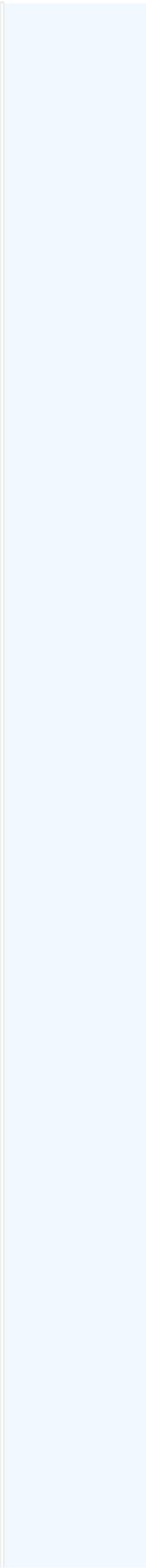
PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	1/25/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 8:	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?	Application programming interfaces (APIs) are the messengers that allow software to

talk to other software. They are the building blocks that allow systems and data to communicate with one another.

The API Manager is a way to manage users, monitor and analyze traffic, promote, and secure APIs with ordered policies. Basically, when an app or API is promoted from one environment to the next level, which includes two or more environments, the fanout behavior can be either of the following: (a) it is promoted simultaneously to all environments that are at the next level or (b) it is promoted to multiple target environments based on custom properties of the app or API. For example, asset-filters might be set up based on one or more custom properties. Furthermore, the API gateway is a management platform as a service (PaaS) that sits between a client and a collection of backend services, and acts as a proxy to allow API calls (automated communications between software), aggregate the various services required to fulfill them and return the appropriate result.

The subject of this privacy impact assessment (PIA) is FDA's use of the MuleSoft Integration Platform as a Service (iPaaS) and API Gateway. MuleSoft is a private sector software company. The platform is equipped with security policies to secure the communication between end points, including Internet Protocol IP (address) Whitelists and Blacklists, hashing and message encryption based on role-based access controls (RBAC) and service level agreements (SLA) defined for each end system. This process is specific to each API system design. For example, if personally identifiable information (PII) data passes through the FDA API Gateway, this would be based on the established RBAC system. The platform and API provide the ability to Hash sensitive data being transmitted such as social security numbers (SSN) for example, hashing renders the data into an unreadable form and prevents unauthorized users from reading the data while also displaying the information to specific/relevant personnel who require the data for their authorized duties.

The API gateway is a conduit for data; it does not store data and does not contain a hard drive or retain permanent memory.



Therefore, MuleSoft does not retain PII or meta data values. The architecture can define a policy to validate or restrict data based on the API requirements.

PTA - 9:

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.

MuleSoft iPaaS API Gateway is not equipped with any type of storage or data element screening capability. Rather, it acts as an integration pass-through between source and destination point, enabling all data to be transmitted or processed through the system. As a pass-through source, MuleSoft iPaaS API Gateway moves data from one system (source system) to another (destination system) and this data may include PII. This can include any type of PII or other data and is currently unknown since Because data is transitioned from multiple source and destination systems, it is not possible to exhaustively identify the data elements transmitted. No transmitted PII is collected and/or stored in the MuleSoft iPaaS API Gateway.

All data is fully encrypted in transit.

FDA conducts separate assessments of source and destination systems, where data is often stored and the data elements can be more specifically identified.

All data is fully encrypted in transit.

FDA conducts separate assessments of source and destination systems, where data is often stored and the data elements can be more specifically identified.

PTA - 10:

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

The MuleSoft iPaaS API Gateway, as used by the FDA, does not store any data. It is merely a conduit for data transmission from the source system/software to a destination system/software. Because the Gateway is employed with many source and destination systems that handle a variety of data, it is not possible to comprehensively describe all of the PII or other data elements transmitted. The general data types and context can range from internal administrative data to regulatory information to research data. The data transmitted is in JSON format, which complies to open web platform industry W3C standards. W3C publishes documents that define Web technologies, and per those standards, PII policies should be discussed for development on a case-by-case basis and not at the platform level.

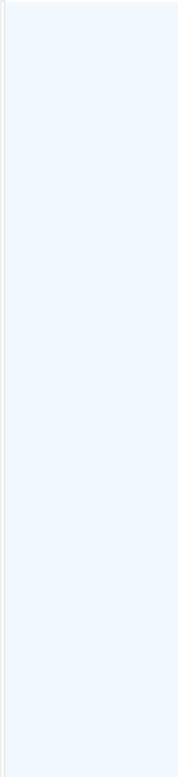
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	Social Security Number
		Truncated SSN
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name
		Driver's License Number
		Mother's Maiden Name
		E-Mail Address
		Phone numbers
		Medical records (PHI)
		Certificates
		Education Records
		Military Status
		Foreign Activities
		Taxpayer ID
		Date of Birth
		Photographic Identifiers
		Biometric Identifiers
		Vehicle Identifiers
		Mailing Address
		Medical Records Number
		Financial Account Info
		Legal Documents
		Devices Identifiers
Employment Status		
Passport Number		
User Credentials		
Patient ID Number		
Others - The API Gateway does not retain PII. It may transmit all manner of data, including PII. Because the Gateway does not store data and is used broadly to shuttle data from numerous sources, it is not possible to exhaustively identify the PII elements transmitted. All PII elements have been selected since types of PII cannot necessarily be determined. PII or other data handled is specific to each API design.		
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies)
		Employees/ HHS Direct Contractors
		Patients
		Public Citizens

		Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
		Other
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	51 - 200
PIA - 4:	For what primary purpose is the PII used?	PII is not used by the MuleSoft API Gateway. The PaaS solely serves a pass-through interface for data between source and destination system(s).
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Other Government Sources Within the OPDIV Other Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet Private Sector Other
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	Notice to PII subjects would be provided to individuals in the context of the source and destination systems where data is maintained and used. FDA personnel and Direct Contractors are notified upon hire of the FDA's creation, collection and use of information about them. FDA's webpages all provide links to FDA's website and privacy policies. This PIA provides additional notice.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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	An opt-out option is not possible, as there is no collection or use of PII data in the MuleSoft API Gateway. Users who wish to opt-out of PII collection must follow protocols identified by the source system and documented in the particular privacy assessment for the source system.
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	The source systems are responsible for providing notice of major changes and obtaining any necessary consent.
PIA - 15:	Describe the process in place to resolve an individual's concerns	Individuals who suspect their PII has been

	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	inappropriately obtained, used or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Systems Management Center (SMC) and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's Systems Management Center (SMC).
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	There is no process in place for periodic reviews of PII as there is no PII data maintained in the system.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Others
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17 Others: Users of MuleSoft API Gateway will not have any access to PII data as PII data is passed through and fully encrypted.	
PIA - 20:	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	All FDA personnel are required to complete FDA's annual IT Security and Privacy Awareness training.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	No additional training is provided to users.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	As no PII is maintained in the API Gateway, there is no applicable records (PII) retention policy or associated processes to retain and destroy PII.
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 role-based access settings, firewalls, passwords and others. Smart cards and Active Directory are used for authentication. Data is encrypted in database per data center requirements. VPN is required when accessing system from remote locations.

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.