

PRIVACY IMPACT ASSESSMENT	
Name of Information System or IT Project:	Vista Health Benefits System
Unique Investment Identifier (Exhibit 53):	485-000000030
System Identifier (3 letter identifier):	VHB
Date:(date the assessment was completed)	May 16, 2016
Indicate whether this PIA is for a new system or for an existing system:	Existing
Purpose of Information System or IT Project:(include if the system is a major application, minor application, or a general support system)	The information System is used to administer a healthcare benefits plan; functions include managing member eligibility for the health benefit and processing health benefit claims. It is considered a Major Application.
Size of the Information System: (approximate number of users for the system)	7000 members
Security Categorization of the System: (e.g. Low, Moderate, High)	Moderate

CONTACT INFORMATION	
Person completing PIA: (Name, title, number, email.)	Todd Sturgeon, Director of Integrated Technologies & CISO 317-655-4608, todd.sturgeon@imglobal.com
Information System Owner: (Name, title, number, email.)	Jennifer Veazey, Program Manager 202-606-6770, jveazey@cns.gov
Information System Security Officer (ISSO): (Name, title, number, email.)	Todd Sturgeon, Director of Integrated Technologies & CISO 317-655-4608, todd.sturgeon@imglobal.com

REVIEWERS	Signature	Date
Information System Owner Jennifer Veazey	Original, signed copy on file with the CNCS OIT cybersecurity office.	5/24/2016
Office of General Counsel Alicia Wilson		
APPROVING OFFICIALS (Contact CNCS by emailing privacy@cns.gov)	Signature	Date
Chief Privacy Officer Amy Borgstrom		
Chief Information Security Officer Stacy Dawn		
Senior Agency Official for Privacy Thomas R. Hanley, Jr.		

SYSTEM APPLICATION/GENERAL INFORMATION

<p>1. Does this system contain any personally identifiable information (PII) about individuals? (Any information collected, maintained, or used that is identifiable to the individual. If the answer is “No,” mark the rest of this document as “N/A.”)</p>	<p>Yes</p>
<p>2. Provide a link to where a list of all the PII data fields are documented within the system and also describe what PII will be collected or maintained by the system. If a link cannot be provided please provide the information in another form. (e.g., First, Middle, Last Name; Social Security Number (SSN); Medical and Health Information; Financial Information; Clearance Information; Date of Birth (DOB); Employment Information; Work Address or Phone Number; Criminal History; Home Address or Phone Number)</p>	<p>The following list documents the PII data fields within the system and as appropriate, descriptions of those data fields have been provided:</p> <ul style="list-style-type: none"> • First Name • Last Name • Start Date of Service Term • End Date of Service Term • Middle Initial • Date of Birth • Gender • Pay Address (including e-mail) • Current Address (including e-mail) • Permanent Address (including e-mail) • Region • All Phone Number Types
<p>3. Is this system identified in the CNCS SORN?</p>	<p>No.</p>
<p>4. Are any modifications of the SORN needed currently?</p>	<p>Yes, modifications are needed; updates are pending.</p>

PII IN THE SYSTEM

<p>5. What categories of individuals are covered in the system? (e.g., public, employees, contractors, grantees, and/or volunteers. Members of the public refers to individuals in a non-employee or non-CNCS contractor context. Members of the public includes individuals for whom CNCS maintains information, as required by law, who were previously employed or contracted by CNCS. PIAs affecting members of the public are posted on the CNCS Privacy page of the public-facing website.)</p>	<p>VISTA Members</p>
<p>6. Why is the PII being collected?</p>	<p>To provide administration management of the health benefit program, management health benefit eligibility and process health benefit claims.</p>
<p>7. How will CNCS use the PII collected? (e.g., SSN are used to track education awards.)</p>	<p>The VHB system uses the PII collected to determine/manage health benefit plan eligibility and process health benefit claims for the individual to whom the PII belongs.</p>

PII IN THE SYSTEM

<p>8. How will the PII be secured?</p>	<ul style="list-style-type: none"> - All electronic data is encrypted at rest and in transit using FIPS 140-2 encryption protocols as well as user Identification with unique passwords, physical firewalls, external certificate authorities, auditing, testing with sanitized data, web application firewall, and FISMA guidelines. Nessus is used for vulnerability scanning and Splunk is used for event correlation and logging. - Data is restricted to authorized users with CNCS roles and permissions; these authorized users have received and passed the required MBI Federal background clearance process. - For physical security: Security guards, close circuit cameras, Proximity ID badges and locked cabinets are used.
<p>9. Is information being obtained from the individual directly? If not directly, then what are the other sources?</p>	<p>Yes, it is collected from the individuals (i.e. VISTA members).</p>
<p>10. Is the PII current? (What steps are being taken to ensure the PII is current and that there is not any PII that needs to be deleted? For example, if someone is no longer an employee, their PII is not needed after a certain point.)</p>	<p>Yes. Members are directed to update information as required; members are directed to the MyAmeriCorps Portal when there is a potential change to any PII.</p>
<p>11. What specific authorities authorize this system or project, the associated collection, use, and/or retention of personal information? (A Federal law, Executive Order of the President or CNCS requirement must authorize the collection. i.e., legal authority to collect SSN.)</p>	<p>Sec. 105 of the Domestic and Volunteer Service Act of 1973, as amended (Pub. L. No. 93-113, as amended) and generally, the Domestic and Volunteer Service Act of 1973, as amended (Pub. L. No. 93-113, as amended)</p>
<p>12. What opportunities do individuals have to decline collection of specific PII/ consent to particular use and/or approve or disapprove of how that information is being shared?</p>	<p>The PII is required for participation in the AmeriCorps VISTA program. While an individual can choose not to provide the information, that individual will be unable to enroll and participate in the AmeriCorps VISTA Program. VISTA members do not otherwise have the ability to opt out or decline the collection of PII.</p>
<p>13. Are the PII elements described in detail and documented? If so, what document provides description? (e.g., Data Management Plan)</p>	<p>Yes, the PII elements are described and documented in detail. The document 44830_Import of Ongoing Eligibility.docx can be found at https://imgsharepoint.olympus.local/EPMO/AmeriCorpsVistaWorksite/Shared%20Documents/44830_Import%20of%20Ongoing%20Eligibility.docx</p>
<p>14. If the information system is operated at more than one site, how will consistency of the information be ensured at all sites?</p>	<p>The system is only operated at one site at a time. The link for the application can be found at: https://americorpsvista.imglobal.com/americorps/HomePage.aspx#LoginBook</p>

MAINTENANCE AND ADMINISTRATIVE CONTROLS

<p>15. What are the retention periods of PII in this system? (This should be consistent with the records schedule as approved by the National Archives and Records Administration.)</p>	<p>All PII and PHI is retained 7 years past the end of the contract or 7 years after individual members are no longer eligible for the health benefit as administered by IMG, whichever is the earliest. At this time, the records shall be destroyed.</p>
<p>16. What are the procedures for disposition of the PII at the end of the retention period?</p>	<p>Physical paper is shredded and recycled. Electronic media is degaussed and destroyed after 7 years</p>
<p>17. Does the system generate audit records containing information that establishes the identity of the individual associated with accessing the system's PII for accountability purposes (e.g., implemented audit logging)? If yes, what information is captured regarding users/usage?</p>	<p>User Identity Logging is captured in the database with modification dates and User ID's where appropriate.</p>
<p>18. Will the PII be retrieved using a personal identifier? List the identifiers that will be used to retrieve information and/or create reports.</p>	<p>Yes, Member info is retrieved within the MyIMGVISTA member portal using a personal identifier. Identifiers used include NSPID (the member's unique ID number issued by CNCS) as well as date of birth.</p>
<p>19. What controls will be used to prevent unauthorized monitoring or retrieval of PII?</p>	<ul style="list-style-type: none"> - All electronic data is encrypted at rest and in transit using FIPS 140-2 encryption protocols as well as user Identification with unique passwords, physical firewalls, external certificate authorities, auditing, testing with sanitized data, web application firewall, and FISMA guidelines. Nessus is used for vulnerability scanning and Splunk is used for event correlation and logging. - Data is restricted to authorized users with CNCS roles and permissions; these authorized users have received and passed the required MBI Federal background clearance process. - For physical security: Security guards, close circuit cameras, Proximity ID badges and locked cabinets are used.

ACCESS TO PII

<p>20. Who will have access to the PII in the system? What kind of access will they have? (e.g., contractors, managers, system administrators, developers, or others. Read only access, read and write access, or change. If contractors have access to the PII in the system, provide evidence that assigned contractors are in compliance with CNCS rules on privacy.)</p>	<ul style="list-style-type: none"> - Contract Users – IMG Employees that have been MBI/CBI cleared; these users have READ, Write, Change access. - System Administrators – IMG Employees that have been MBI/CBI cleared (received/passed a required federal background investigation). These users have READ, Write, Change access. - Developer - IMG Employees that have been MBI/CBI cleared (received/passed a required federal background investigation); these users have READ, Write, Change access. - VISTA Members – people that have access via the IMG VISTA Portal; these users have READ, Write, Change access for their own personal files, but do not have access to other VISTA member's data or files.
---	--

ACCESS TO PII

<p>21. What controls are in place to prevent the misuse of PII by those having access and who is responsible for assuring proper use of the PII? (Please list processes and training materials.)</p>	<p>Annual Security Awareness training for all IMG employees and staff. Specific Security Awareness training for those involved in the processing of AmeriCorps data. Compartmentalization/restrictions on what data can be viewed based on a user's assigned rights. The ISSM and his designees are responsible for assuring proper use of the PII.</p>
<p>22. Who will the PII be shared with? List other systems that share or have access to the PII. If other systems have access to or share the PII, is there an interconnection agreement in place or written agreement regarding the sharing and how the PII will be protected? How will the PII be used by the other agency and who will be responsible for protecting the privacy rights of the public and employees affected by any interface?</p>	<p>IMG has contracts with Equian and Universal RX to process specific claims per CNCS recommendations; work/agreements outlined within documented Business Associate Agreements. Necessary data is shared with business partners via a Secure FTP. There is not an interconnection agreement as IMG does not directly interface with either system. We intentionally abstract this for security purposes. Additional Member Services will be provided by both of these entities.</p>
<p>23. Will the information be saved to removable media, or printed to hard copy? How will removable media and or hard copies be protected?</p>	<p>No.</p>