

PRIVACY IMPACT ASSESSMENT	
<b>Name of Information System or IT Project:</b>	NCCC Health Benefit System, Part of the Seven Corners Information System
<b>Unique Investment Identifier (Exhibit 53):</b>	485-000000023
<b>System Identifier (3 letter identifier):</b>	NHB
<b>Date:(date the assessment was completed)</b>	May 16, 2016
<b>Indicate whether this PIA is for a new system or for an existing system:</b>	Existing
<b>Purpose of Information System or IT Project:(include if the system is a major application, minor application, or a general support system)</b>	<p>Major Application</p> <p>The NCCC Health Benefit System, part of the Seven Corners Information System, assists Seven Corners to provide health benefit services to NCCC Members. The system supports the following business functions regarding the health care provisioning and payment of health care claims for NCCC Members:</p> <ul style="list-style-type: none"> <li>• Membership / Eligibility tracking</li> <li>• Claim entry</li> <li>• Claims adjudication</li> <li>• Claim re-pricing</li> <li>• Claim payment</li> <li>• Invoicing</li> <li>• Policy Administration</li> <li>• Program reporting</li> </ul>
<b>Size of the Information System:</b> (approximate number of users for the system)	2100 NCCC Members
<b>Security Categorization of the System:</b> (e.g. Low, Moderate, High)	Moderate

CONTACT INFORMATION	
<b>Person completing PIA:</b> (Name, title, number, email.)	Christopher Pawley, ISSO Director Technical Services 317-575-2652 x3339 <a href="mailto:Chris.pawley@sevencorners.com">Chris.pawley@sevencorners.com</a> Seven Corners Information Systems
<b>Information System Owner:</b> (Name, title, number, email.)	Jennifer Veazey Program Manager 202-606-6770 <a href="mailto:jveazey@cns.gov">jveazey@cns.gov</a>
<b>Information System Owner:</b> (Name, title, number, email.)	Ryan Brubaker Chief Information Officer 317-575-2652 ext. <a href="mailto:Ryan.brubaker@sevencorners.com">Ryan.brubaker@sevencorners.com</a> Seven Corners Information Systems
<b>Information System Security Officer (ISSO):</b> (Name, title, number, email.)	Christopher Pawley, ISSO Director Technical Services 317-575-2652 x3339 <a href="mailto:Chris.pawley@sevencorners.com">Chris.pawley@sevencorners.com</a> Seven Corners Information Systems

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

SYSTEM APPLICATION/GENERAL INFORMATION	
<b>1. Does this system contain any personally identifiable information (PII) about individuals?</b> (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.")	Yes
<b>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.</b> (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)	The following list documents the PII data fields within the system and as appropriate, descriptions of those data fields have been provided:  Member ID (this is a unique system generated and assigned ID number); SSN; Member Address; Member Birthdate; Member Name (First and Last); Diagnosis or Nature of the Illness; Medical Claim Information including the following: Date of Service for the claim; Amount of the claim.
<b>3. Is this system identified in the CNCS SORN?</b>	No.
<b>4. Are any modifications of the SORN needed currently?</b>	Yes, modifications are needed; updates are pending.

PII IN THE SYSTEM	
<b>5. What categories of individuals are covered in the system?</b> (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.)	NCCC Members
<b>6. Why is the PII being collected?</b>	To provide administration management of the health benefit program, management health benefit eligibility and process health benefit claims.
<b>7. How will CNCS use the PII collected?</b> (e.g., SSN are used to track education awards.)	The PII collected will be used to determine/manage health benefit plan eligibility and process health benefit claims for the individual to whom the PII belongs.
<b>8. How will the PII be secured?</b>	Users have to have unique username and password to access system. 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. Data is encrypted both at rest and in transit.
<b>9. Is information being obtained from the individual directly? If not directly, then what are the other sources?</b>	Yes, it is collected from the individuals (i.e. NCCC members).
<b>10. Is the PII current?</b> (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.)	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.
<b>11. What specific authorities authorize this system or project, the associated collection, use, and/or retention of personal information?</b> (A Federal law, Executive Order of the President or CNCS requirement must authorize the collection. i.e., legal authority to collect SSN.)	Section 158 of the National and Community Service Act of 1990, as amended (Pub. L. No. 101-610, as amended), and the National and Community Service Act of 1990
<b>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?</b>	NCCC members do not have the ability to opt out or decline the collection of PII; if a member does opt into providing PII, the members are unable to enroll into and participate in the AmeriCorps NCCC Program.

PII IN THE SYSTEM	
13. Are the PII elements described in detail and documented? If so, what document provides description? (e.g., Data Management Plan)	The NHB AXIS Core Design Document documented as(NHB_Artifact 040) is a detailed description of the system used to manage member health benefit eligibility and process health benefit claims. The design document includes an outline of the PII elements collected within the system as well as their descriptions. The above referenced artifact is an internal document accessible to both Seven Corners and CNCS.
14. If the information system is operated at more than one site, how will consistency of the information be ensured at all sites?	The NHB only operates at one site. 303 Congressional Blvd., Carmel, IN 46032. The link for the application can be found at: <a href="https://member.sevencorners.com/Account/Login">https://member.sevencorners.com/Account/Login</a>

MAINTENANCE AND ADMINISTRATIVE CONTROLS	
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.)	10 years past the end of the contract or 10 years after individual members are no longer eligible for the health benefit as administered by Seven Corners, whichever is the earliest. At this time, the records shall be destroyed.
16. What are the procedures for disposition of the PII at the end of the retention period?	<p>All data is stored in the NHB application database. It is kept encrypted at rest and in transit. Data is kept for ten years past the end of the contract.</p> <p>At the point where the retention period expires (10 years following the contract expiration date) data will be deleted from the system as detailed below. Method for destruction depends on the method in which the information is stored:</p> <p><b>Paper Records</b> - Place documents in a secure container bound for shredding by a company with current certification from the National Association for Information Destruction (NAID).</p> <p><b>Electronic records saved in the system</b> - After a Seven Corners administrator with permissions deletes a database record using tested SQL scripts, and confirms deletion of that item, the data in question is removed and no longer accessible from any user's interface. The data is then deleted from the active servers and replication servers. Pointers to the data on active and replication servers are removed. Dereferenced data will be overwritten with other customer data over time.</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?	The system generates audit records for changes but not for access. Each record shows the system generated USERID of the user who made the action. In addition to audit logging, each data element is marked with the USERID and DATETIME of the most recent edit, which could be creation.

MAINTENANCE AND ADMINISTRATIVE CONTROLS	
18. Will the PII be retrieved using a personal identifier? List the identifiers that will be used to retrieve information and/or create reports.	Yes. Individual Member User Names
19. What controls will be used to prevent unauthorized monitoring or retrieval of PII?	Users have to have a username and password to access system. Data is restricted to only users with CNCS roles and permissions. Only Seven Corners staff users who have received and passed a MBI clearance level Federal background check are authorized to access the system.

ACCESS TO PII	
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.)	Access to PII is limited to Seven Corners' contractors who have access to read/write within the system, as well as members who have access to read their own information within the system. All Seven Corners' contractor users have undergone Computer Security Training as part of the Onboarding Process. Training documents include: Seven Corners IT Security Policy, Seven Corners Corporate Information Protection Policy and the Seven Corners Acceptable Use Policy.

<p>. <b>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?</b> (Please list processes and training materials.)</p>	<p><b>Seven Corners Corporate Acceptable Use Policy</b> - This document is our official Acceptable Use Policy (AUP). It explains what behaviors and uses are acceptable or unacceptable in order to help protect our services, our customers, and the Internet community from irresponsible or illegal activities.</p> <p><b>Seven Corners Corporate System Documentation policy</b> - This policy explains the strategy followed by Seven Corners departmental areas regarding document management. The guidelines outlined in this policy will be used to guide the administration, approval, maintenance and handling of electronic files to ensure consistency in delivery and demonstrate appropriate controls.</p> <p><b>Seven Corners IT Access Security Policy</b> - This document outlines how access to NHB data will be managed by the Seven Corners Information Technology department.</p> <p><b>Seven Corners IT Application Source Code Review Procedure</b> - This document defines the procedure for reviewing custom-developed source code for the NHB claim processing application.</p> <p><b>Seven Corners IT Audit and Accountability Policy</b> - The purpose of this policy is to ensure that there is adequate tracking of all access, alterations and deletions to NHB data. Entities affected by this policy include any individual, group or department that owns, operates or maintains information resources on the Seven Corners computer network.</p> <p><b>Seven Corners IT AXIS Core Security Plan and Administration</b> - The plan describes the physical and logical security related requirements and controls for the NHB Claim Processing system.</p> <p><b>Seven Corners IT Change Control Policy</b> – defines the processes and procedures for changes to Information Technology resources (e.g., computer hardware, computer software, operating systems, applications, database, data, network, security, and telecommunications). It is the intention that changes occur in a rational and predictable manner and within a controlled environment, so that planning can occur accordingly. In addition, the standard serves as a vehicle for identifying, communicating, planning, testing, approving, implementing, and documenting changes to Seven Corners’ Information Technology resources.</p> <p><b>Seven Corners IT Continuous Monitoring Policy</b> – defines the requirements for using tools such as metrics, assessments, event monitoring, data analysis, response and reporting to ensure the security of the NHB data on the Seven Corners network.</p> <p><b>Seven Corners IT Data Transmission Policy for the NCCC Health Benefit System</b> - describes Seven Corners’ standards for securing and sending NHB data.</p> <p><b>Seven Corners IT Flaw Remediation Policy</b> - addresses the intrinsic faults and weaknesses in software and establishes</p>
---	--

	<p>the necessary measures that should be taken to mitigate the risk of exploitation within the Seven Corners' information system.</p> <p><b>Seven Corners IT Hardware/Software Configuration</b> - describes the baseline for IT software and hardware configuration at Seven Corners.</p> <p><b>Seven Corners IT Incident Management Policy</b> – establishes incident response capability throughout Seven Corners and its business units for identifying, responding to and managing Information incidents involving security, system crashes and threats to physical and logical security which may occur across the enterprise environment.</p> <p><b>Seven Corners IT Incident Management Process</b> – defines the process steps to be taken in the event of an incident related to NHB data.</p> <p><b>Seven Corners IT Incident Response Test Plan</b> - describes the testing activity for testing Seven Corners' Incident Management policy and procedures.</p> <p><b>Seven Corners IT NHB Interconnections</b> - describes the interconnections between the Seven Corners NHB system and the applications it interacts with in the course of daily business activities.</p> <p><b>Seven Corners IT Kerberos Protocol</b> – describes the use of the Kerberos distributed authentication service as a method of authentication on the Seven Corners network.</p> <p><b>Seven Corners IT Principle of Least Access Privilege</b> –describes company policy of minimal user profile privileges on computers, based on the users' job necessities.</p> <p><b>Seven Corners IT Media Sanitation Policy</b> - defines the requirements for ensuring data are permanently removed from media before disposal or reuse, and properly disposing of media.</p> <p><b>Seven Corners IT NCCC Network Application Session Policy</b> - defines session logout, lockout and termination as it applies to NHB data.</p> <p><b>Seven Corners IT Periodic Review Procedure</b> – defines the procedure for performing post-implementation periodic reviews.</p> <p><b>Seven Corners IT Physical/Logical Security Policy</b> - defines policies and procedures to protect NHB data from credible threats, whether internal or external, deliberate or accidental. Also outlines the framework and addresses security issues related to the confidentiality, integrity and availability of NHB data housed in Seven Corners' IT systems.</p> <p><b>Seven Corners IT Risk Analysis Policy</b> – describes process and defines requirements for discovering risks and threats to the NHB system and provides detail on implementing prevention measures to mitigate or to reduce the risks. Provides guidance on how to conduct a Risk Analysis, evaluate and analyze the information that is collected, and implement appropriate strategies that will help the organization to manage the potential risks.</p>
--	---

	<p><b>Seven Corners IT Roles and Responsibility Policy</b> - defines the roles and responsibilities for the Seven Corners Information Technology department with regard to Information Security as it applies to NHB data.</p> <p><b>Seven Corners IT Incident Response Plan</b> - addresses how Seven Corners' will respond to any breaches to the computer systems, sensitive and/or confidential NHB data.</p> <p><b>Seven Corners IT Security/PI Incident Report Form</b> – used to report instances of Security breach as it applies to the Seven Corners Information System and NHB data.</p> <p><b>Seven Corners IT Security Policy</b> - describes the manner in which the Seven Corners Information Technology department monitors, secures and protects information, systems, programs, physical environment, etc. used in normal business activities from loss and unauthorized access, modification, disclosure, inappropriate alteration or misuse.</p> <p><b>Seven Corners IT Separation of Duties Policy</b> - outlines the framework for the Separation of Duties within the IT organization.</p> <p><b>Seven Corners IT Software Configuration Management Access Security</b> – an addendum to the Software Configuration management plan that describes access security for Visual Studio Online used by the Application Development team as a development configuration management tool for NHB data.</p> <p><b>Seven Corners IT NHB System Documentation Policy</b> - establishes the policy and procedures for the development, maintenance, and regular review of Seven Corners information system documentation.</p> <p><b>Seven Corners IT System Maintenance Policy</b> - establishes the policy for managing risks including information asset maintenance and repairs through the establishment of an effective System Maintenance program.</p> <p><b>Seven Corners IT Vulnerability Assessment Policy</b> - defines the policy on scanning for and remediating vulnerabilities on all Seven Corners networked computing devices.</p> <p><b>Seven Corners Privacy Policy</b> - describes how Seven Corners manages and safeguards NHB privacy information and data gathered in the course of doing business.</p> <p><b>Seven Corners Remote Access Policy</b> - define rules and requirements for connecting to Seven Corners' network from an external workstation.</p> <p><b>Seven Corners Security Planning Policy</b> - establishes process and procedures, aligned with applicable Seven Corners security policy and standards, to ensure the Seven Corners IT develops, disseminates, and updates the Seven Corners System Security Plan.</p> <p><b>Seven Corners User Access Review Process</b> – Describes the Seven Corners IT process for reviewing all users with access to the NHB system. Seven Corners conducts quarterly User Access Reviews to actively monitor and verify the appropriateness of a users' access to systems and applications based on an</p>
--	--

ACCESS TO PII	
	understanding of the minimum necessary for users to perform or support business activities or functions.
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?	Seven Corners has repricing contracts with re-pricing vendors as well as Non-Disclosure Agreements and Business Associate Agreements. Claims in the NHB system are shared with a repricing vendor (Equian) for the purposes of obtaining the best cost per medical procedure based on network discounts. In order for Equian to process the claim discount they require the full details of the claim which includes PII of the claimant. Seven Corners maintains Business Associate Agreements and a Non-Disclosure Agreement with Equian. By contract Equian is required to maintain data security and privacy as well as adhere to all HIPAA requirements. All transmissions between Seven Corners and Equian are via SFTP using PGP encryption. Seven Corners does not use an MOU. A Business Associate Agreement is used instead. The Business Associate Agreement in the form of <b>NHB_Artifact 234 – SC_CORP_HITECHBAA</b> is available internally to CNCS and Seven Corners staff.
23. Will the information be saved to removable media, or printed to hard copy? How will removable media and or hard copies be protected?	No

**Commented [VJD1]:** CNCS should obtain a copy of Seven Corners MOU/Business Agreements with these sub-contractors and these subs/processes should be outlined in the SSP. Follow up on this one.

**Commented [RAH2R1]:** Response revised to answer questions.