




## 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

<b>PIA Name:</b>	CDC - HEHR - QTR2 - 2024 - CDC8292827	<b>PIA ID:</b>	1917011
<b>Name of Component:</b>	CDC - Healthcare Electronic Health Records	<b>Name of ATO Boundary:</b>	Healthcare Electronic Health Records
<b>Overall Status:</b>		<b>PIA Queue:</b>	
<b>Submitter:</b>		<b># Days Open:</b>	89
<b>Submission Status:</b>	Re-Submitted	<b>Submit Date:</b>	6/17/2024
<b>Next Assessment Date:</b>	08/28/2027	<b>Expiration Date:</b>	8/28/2027
<b>Office:</b>		<b>OPDIV:</b>	CDC
<b>Security Categorization:</b>		<b>OpDiv PIA ID:</b>	CDC8292827
<b>Legacy PIA ID:</b>		<b>Make PIA available to Public?:</b>	Yes
<b>1:</b>	Identify the Enterprise Performance Lifecycle Phase of the system.		Operations and Maintenance
<b>2:</b>	Is this a FISMA-Reportable system?		Yes
<b>3:</b>	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		Yes
<b>4:</b>	ATO Date or Planned ATO Date.		8/19/2024
<b>5:</b>	Is the system or electronic information collection, agency or contractor operated?		Agency

## PTA

### PTA

<b>PTA - 2:</b>	Indicate the following reason(s) for this PTA. Choose from the following options.	New
<b>PTA - 2A:</b>	Describe in further detail any changes to the system that have occurred since the last PIA.	
<b>PTA - 3:</b>	Is the data contained in the system owned by the agency or contractor?	Agency
<b>PTA - 4:</b>	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.	Healthcare Electronic Health Records (HEHR) system provides technical support to CDC's Division of Health Care Statistics (DHCS) in implementation of the public health registry component of the National Health Care Surveys (NHCS) (a family of nationally representative surveys of health care providers in inpatient, outpatient, ambulatory, and long-term care settings) and to support the receipt of data from Eligible Professionals (EPs) in accordance with the Meaningful Use (MU) Program rules. The scope of this project includes infrastructure planning and maintenance, developing the surveys registry portal to allow for registration of hospitals and providers that intend to participate in the survey.
<b>PTA - 5:</b>	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.	<b>Registration Portal:</b> Provides authentication, authorization, and auditing for internal and external CDC users to

interact with a subset of business/public use records. Administering and automating the processes serving the Promoting Interoperability hospital relationships of the DHCS. Registration Portal can be accessed at the following URL: <https://hehr.nchs.cdc.gov/registrations-ui/#/login>

Registration Portal consists of the following components:

1. Registrar (user account) creation and maintenance including easy self-registration, ability to reset expired passwords without involving an admin user.
2. Hospital Registration (add, edit, submit, withdraw, and validate).
3. Provider Registration (add, edit, submit, withdraw, and validate).
4. Group Registration (add, edit, submit, withdraw, and validate).
5. Ability of a registrar to manage large numbers of hospitals, groups, and providers by:
  - a. Organization of registered entities into logical groups that are akin to “folders” on a computer.
  - b. Add, edit, organize, and remove registrations via bulk upload.
  - c. Search registrations.
  - d. Transfer registrations from one registrar to another.
  - e. Delegate registration authority from one registrar to another.
6. Frequently Asked Questions (FAQ) information.
7. Ability to contact the helpdesk via a webform with a pre-selected set of topics/subjects (“Contact Us.”).
8. View Correspondence such as AAEVD letters or other communications sent out by the system to the Registrar.
9. Annual Active Engagement Verification Document (AAEVD) letter generation.

The following types of information will be collected and stored:

- 1) Username and Password
- 2) HEHR registration data for providers and hospitals like provider name, address, contact information, provider type and specialty.
- 3) Hospital-level data – Hospital characteristics (e.g., ownership status, total admissions, and total births) are collected through the Annual Hospital Interview.
- 4) Sampled hospital information – identification of a hospital as being selected for a survey.
- 5) Patient data – All inpatient discharges and Emergency Department (ED) visits through collection of electronic health records, administrative claims, or state files (e.g., Patient’s full name, address, Social Security Number (SSN), medical record number, date of birth, sex, race, marital status, type of care, date\time of

admission/visit/arrival/departure/discharge, triage system\level, mode of arrival, point of origin, cause of injury, discharge disposition, lab test, diagnosis, expected source of payment, National Provider Identifier of physicians, and number of days of care).

**PTA - 5A:** Are user credentials used to access the system?

**PTA - 5B:** Please identify the type of user credentials used to access the system.

Non-HHS User Credentials

Username

Password

**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.

HEHR collects patient-level PII, such as Patient Name and Social Security Number, in order to create patient identifiers that will allow for data linkage between settings (i.e., Inpatient, Emergency Department, Outpatient Department) time (i.e., year to year linkages), and data collections (e.g., link to the National Death Index to construct 30-day mortality indicators.

1) Username and Password - Authentication to HEHR Registration Portal

2) HEHR registration data - User registration information for providers and hospitals (provider name, address, contact information, provider type and specialty)

3) Hospital-level data – Hospital characteristics are collected through the Annual Hospital Interview.

Hospitals are asked to complete the AHI to create national estimates on hospital care and utilization.

AHI request hospitals to provide summary information on emergency department, outpatient department and inpatient department visits for the calendar year.

This information will be used for statistical purposes and for further insight on sampled hospitals.

(ownership status, total admissions, and total births)

4) Sampled hospital information – identification of a hospital as being selected for a survey. In order for policy makers to form solid, evidence-based decisions about health care in the U.S. it is essential that we collect nationally representative data on hospital utilization. This information will be used for statistical purposes.

5) Patient data – All inpatient discharges and Emergency Depart (ED) visits through collection of electronic health records, administrative claims, or state files (e.g., Patient’s full name, address, Social Security Number (SSN), medical record number, date of birth, sex, race, marital status, type of care, date\time of admission/visit/arrival/departure/discharge, triage system\level, mode of arrival, point of origin, cause of injury, discharge disposition, lab test, diagnosis, expected source of payment, National Provider Identifier of physicians, and number of days of care). In order for policy makers to form solid, evidence-based decisions about health care in the U.S. it is essential that we collect nationally representative data on hospital utilization. This information will be used for statistical purposes.

**PTA - 7:**

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

Yes

<b>PTA - 7A:</b>	Does this include Sensitive PII as defined by HHS?	Yes
<b>PTA - 8:</b>	Does the system include a website or online application?	Yes
<b>PTA - 8A:</b>	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
<b>PTA - 9:</b>	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.	HEHR Registration Portal enables Eligible Clinicians (ECs), Eligible Professional (EPs), Eligible Hospitals (EHs) and Critical Access Hospitals (CAHs) to register their intent to submit data to the National Health Care Surveys as part of their participation in Promoting Interoperability (PI) and the Merit-based Incentive Payment System (MIPS).
<b>PTA - 10:</b>	Does the website have a posted privacy notice?	Yes
<b>PTA - 11:</b>	Does the website contain links to non-federal government websites external to HHS?	No
<b>PTA - 11A:</b>	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
<b>PTA - 12:</b>	Does the website use web measurement and customization technology?	Yes
<b>PTA - 12A:</b>	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
<b>PTA - 13:</b>	Does the website have any information or pages directed at children under the age of thirteen?	No
<b>PTA - 13A:</b>	Does the website collect PII from children under the age thirteen?	
<b>PTA - 13B:</b>	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?	
<b>PTA - 14:</b>	Does the system have a mobile application?	No
<b>PTA - 14A:</b>	Is the mobile application HHS developed and managed or a third-party application?	
<b>PTA - 15:</b>	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
<b>PTA - 16:</b>	Does the mobile application/ have a privacy notice?	
<b>PTA - 17:</b>	Does the mobile application contain links to non-federal government websites external to HHS?	
<b>PTA - 17A:</b>	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
<b>PTA - 18:</b>	Does the mobile application use measurement and customization technology?	
<b>PTA - 18A:</b>	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
<b>PTA - 19:</b>	Does the mobile application have any information or pages directed at children under the age of thirteen?	
<b>PTA - 19A:</b>	Does the mobile application collect PII from children under the age thirteen?	
<b>PTA - 19B:</b>	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?	
<b>PTA - 20:</b>	Is there a third-party website or application (TPWA) associated with the system?	No
<b>PTA - 21:</b>	Does this system use artificial intelligence (AI) tools or technologies?	No

**PIA**

<b>PIA</b>		
<b>PIA - 1:</b>	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	<p>Social Security Number</p> <p>Name</p> <p>Email Address</p> <p>Phone numbers</p> <p>Date of Birth</p> <p>Mailing Address</p> <p>Medical Records Number</p> <p>User Credentials</p> <p>Patient ID Number</p> <p>Other - Free text Field - Medical notes, demographic information such as sex and race. Marital status.</p>
<b>PIA - 2:</b>	Indicate the categories of individuals about whom PII is collected, maintained or shared.	<p>Patients</p> <p>Members of the public</p>
<b>PIA - 3:</b>	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
<b>PIA - 4:</b>	For what primary purpose is the PII used?	<p>HEHR collects patient-level PII, such as Patient Name and Social Security Number, in order to create patient identifiers that will allow for data linkage between settings (i.e., Inpatient, Emergency Department, Outpatient Department) time (i.e., year to year linkages), and data collections (e.g., link to the National Death Index to construct 30-day mortality indicators.</p>
<b>PIA - 5:</b>	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	<p>HEHR collects physician name, address, and National Provider Identifier number in order to verify physician information and to link HEHR data with external data sources.</p> <p>Further, once data has been linked, various analysis could possibly be conducted for research purposes.</p>
<b>PIA - 6:</b>	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	<p>SSN is part of data submitted and required for data analysis. SSNs are used for merging data (or linking with other data sources)</p>
<b>PIA - 6A:</b>	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	EXECUTIVE ORDER 9397 NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS
<b>PIA - 7:</b>	Identify legal authorities governing information use and disclosure specific to the system and program.	<p>Public Health Service Act, Section 306(b) (42 U.S.C. 242k)</p> <p>Public Health Service Act, Title 42, US Code, Paragraph 242k - National Center for Health Statistics.</p>
<b>PIA - 8:</b>	Are records in the system retrieved by one or more PII data elements?	Yes

<b>PIA - 8A:</b>	Please specify which PII data elements are used to retrieve records.	<p>1. Name: Patient First and last names, and sometimes middle names or initials.</p> <p>2. Social Security Number (SSN): A unique identifier</p> <p>3. Date of Birth (DOB): Patient birth date</p> <p>4. Address: Patient current and previous addresses, such as street, city, state, and ZIP code.</p>
<b>PIA - 8B:</b>	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.	<p>SORN 09-20-0167 System Name: Health Resources Utilization Statistics, HHS/OASH/NCHS</p> <p><a href="https://www.hhs.gov/foia/privacy/sorns/09200167/index.html">https://www.hhs.gov/foia/privacy/sorns/09200167/index.html</a></p>
<b>PIA - 9:</b>	Identify the sources of PII in the system.	<p>Directly from an individual about whom the information pertains</p> <p>Email</p> <p>Online</p>
<b>PIA - 10:</b>	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
<b>PIA - 10A:</b>	Provide the information collection approval number.	OMB Number: 0920-0212
<b>PIA - 10B:</b>	Identify the OMB information collection approval number expiration date.	12/31/2024
<b>PIA - 10C:</b>	Explain why an OMB information collection approval number is not required.	N/A
<b>PIA - 11:</b>	Is the PII shared with other organizations outside the system's Operating Division?	No
<b>PIA - 11A:</b>	Identify with whom the PII is shared or disclosed.	
<b>PIA - 11B:</b>	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
<b>PIA - 11C:</b>	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)).	
<b>PIA - 11D:</b>	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.	
<b>PIA - 12:</b>	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
<b>PIA - 12A:</b>	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
<b>PIA - 13:</b>	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.	There is no method for individuals to opt-out of the collection or use of their PII. The Public Health Service Act, Title 42 permits disclosure of protected health information without patient authorization for 1) public health purposes and 2) research that has been approved by an Institutional Review Board (IRB)

<b>PIA - 14:</b>	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.	CDC/NCHS does not collect nor is it provided information that will allow for notifications to occur; no contact information is made available.
<b>PIA - 15:</b>	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.	In the event that a patient requests information about disclosures of their protected health information, hospitals are required to keep Accounting Documentation for 6 years. NCHS has developed an accounting document for NHCS hospitals that allows a hospital to respond to requests by patients for disclosures made of their protected health information. A separate accounting document will be provided to hospitals to simplify their record-keeping and for their convenience in complying with this requirement.
<b>PIA - 16:</b>	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.	<p>HEHR is a one-way data collection and consolidation process. HEHR relies on the accuracy of the source hospital systems. There is no feedback loop that allows for the accuracy of the data to be validated.</p> <p>HEHR measures completeness of healthcare data received from hospitals. Data is reviewed for completeness on a continuous basis. NCHS is currently developing procedures for quarterly reporting to define data elements.</p> <p>DHCS designated staff annually reviews all DHCS production system data to make sure it remains in compliance with strict controls required by the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) legislation and annual risk assessments are conducted as part of the Security Certification and Accreditation Review and the DHHS Information Security Program Policy.</p>
<b>PIA - 17:</b>	Identify who will have access to the PII in the system.	Administrators Others
<b>PIA - 17A:</b>	Select the type of contractor.	
<b>PIA - 17B:</b>	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
<b>PIA - 18:</b>	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	<p>Administrators: A limited number of users support the registration and survey management.</p> <p>Others: A limited number of database analysts have access to perform data integration and testing. Operations team members work directly with hospitals to set up and support participation in the survey and evaluation data received. Data integration analysts/developers work with the data for standardization and integration purposes.</p>

<b>PIA - 19:</b>	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	CDC Policy establishes procedures for users to request access to PII data based on position description or contract responsibilities. The NCHS Rules of Behavior governs the appropriate use of NCHS CIPSEA data as defined by this document, applicable CDC Policy.
<b>PIA - 20:</b>	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.	Authorization to PII data must be approved utilizing the Division of Health Care Statistics (DHCS) Data Access Request Form. Access to PII for must be approved by the immediate supervisor, Branch Chief and NCHS Data Owner.
<b>PIA - 21:</b>	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.	NCHS Users complete mandatory Security Awareness Training annually in accordance with CDC/NCHS policy.
<b>PIA - 22:</b>	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users must sign an annual NCHS Confidentiality Non-Disclosure Affidavit, complete the annual mandatory NCHS Confidentiality Training.
<b>PIA - 23:</b>	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 disposed of according to the CDC Records Control Schedule for Scientific and Research Project Records N1-442-09-1. The permanent records are electronically transferred to the National Archives and Records Administration (NARA) in accordance with N1-442-09-1,1.
<b>PIA - 24:</b>	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	<p>Administrative controls: documented policies and procedures and non-disclosure agreements that CDC employees agree to adhere to upon hire and annually thereafter, annual security awareness training, Role-Based training, minimum necessary Role-Based access, monitoring of access logs and user activities, established data disposition procedures, periodic correspondence with CDC staff to reinforce confidentiality regulations, guidelines, and procedures.</p> <p>Technical controls: access restrictions based on least privilege and need to know, Role-Based access managed by CDC AD, User ID/Password, and ID cards, virus/malicious code detection software, firewalls, virtual private network, intrusion detection system, database backups, and data encryption.</p> <p>Physical controls: building guards, identification badges, key cards, closed circuit TV, and locked offices.</p>

## Review & Comments

### Privacy Analyst Review

<b>OpDiv Privacy Analyst Review Status:</b>	Approved	<b>Privacy Analyst Review Date:</b>	6/18/2024
<b>Privacy Analyst Comments:</b>	OpDiv Analyst: Joshua Mosios (Contractor)	<b>Privacy Analyst Days Open:</b>	

### SOP Review

<b>SOP Review Status:</b>	Approved	<b>SOP Signature:</b>	
<b>SOP Comments:</b>	Approved on behalf of Beverly Walker	<b>SOP Review Date:</b>	7/15/2024
		<b>SOP Days Open:</b>	28

### Agency Privacy Analyst Review

<b>Agency Privacy Analyst Review Status:</b>	Approved	<b>Agency Privacy Analyst Review Date:</b>	7/19/2024
<b>Agency Privacy Analyst Review Comments:</b>	Reviewer: Crystal Bland This PIA had a few minor comment but is ready for SAOP review and approval.	<b>Agency Privacy Analyst Days Open:</b>	4

### SAOP Review

<b>SAOP Review Status:</b>	Approved	<b>SAOP Signature:</b>	Archer Signature_Bridget Guenther.docx
<b>SAOP Comments:</b>	<p>There are a number of updates that need to be made for the next iteration. Once the PTA fix is implemented, I recommend CDC make these corrections so the PTA and PIA are consistent:</p> <p>Reviewer noted that on the Component PTA the ATO date is 8/24/2024 but on the Dashboard PTA ATO is 8/19/2024.</p> <p>On the next iteration of the PTA:</p> <p>PTA-5: Add "medical notes" as PII collected, maintained, stored in the system.</p> <p>PIA-1 Include Provider Type, Physician's Name, and National Provider Identifier (NPI) as PII elements listed.</p>	<b>SAOP Review Date:</b>	8/28/2024
		<b>SAOP Days Open:</b>	40

### Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

## Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	6/17/2024	Please de-select "Medical Records (PHI)" and select "Medical Records Number". Additionally, include "medical notes and demographic information such as sex and race". Additionally, select "User Credentials" and "Marital Status"	
PIA - 8A	Data Feed Service, piafrmcdc	6/17/2024	Please modify answer. Not all of these elements fit the definition of direct personal identifiers.	
PIA - 16	Data Feed Service, piafrmcdc	6/17/2024	Define all acronyms upon first use (CIPSEA)	
PIA - 21	Data Feed Service, piafrmcdc	6/17/2024	Note the frequency of training.	
PIA - 1	BLAND, CRYSTAL	7/19/2024	<p>Reviewer noted that on the Component PTA the ATO date is 8/24/2024 but on the Dashboard PTA ATO is 8/19/2024.</p> <p>On the next iteration of the PTA:</p> <p>PTA-5: Add "medical notes" as PII collected, maintained, stored in the system.</p> <p>PIA-1 Include Provider Type, Physician's Name, and National Provider Identifier (NPI) as PII elements listed.</p>	

## Admin Section

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

## Miscellaneous Fields

Last Updated:	8/28/2024 8:01 PM	History Log:	<a href="#">View History Log</a>
---------------	-------------------	--------------	----------------------------------