Save

Privacy Impact Assessment Form

v 1.21

Status | Form Number | Form Date 12/05/2023

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	TBD
2a	Name:	National Healthcare Safety Network (Cloud) (NHSN2)
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ◉ Major Application ○ Minor Application (stand-alone) ○ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Development
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	○ Yes ◉ No
5	Identify the operator.	◉ Agency ○ Contractor
6	Point of Contact (POC):	POC Title: Branch Chief POC Name: Andrea Benin POC Organization: NCEZID/DHQP POC Email: aqb4@cdc.gov POC Phone: 404-498-1186
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	12/1/2023 ☐ Not Applicable

Save

8c	Briefly explain why security authorization is not required	N/A	
10	Describe in further detail any changes to the system that have occurred since the last PIA.	The National Healthcare Safety Network (Cloud) (NHSN2) is a cloud-based system migrated from the National Healthcare Safety Network (NHSN) on-prem system, which has an approved PIA. Migration to the cloud is a significant system management change which will result in new privacy risks.	
11	Describe the purpose of the system.	The National Healthcare Safety Network (Cloud) (NHSN2) is a cloud-based system migrated from the National Healthcare Safety Network (NHSN) system. The major purpose of NHSN2 is to equip participating healthcare facilities to enter data associated with healthcare safety events, such as surgical site infections, anti-microbial use and resistance, bloodstream infections, and healthcare worker vaccinations. NHSN2 provides analysis tools that generate reports using the aggregated data (reports about infection rates, national and local comparisons, etc.). Participating NHSN2 healthcare facilities can access web-based screens that allow them to enter data associated with healthcare safety events. These data are captured in a relational database at the CDC. Participants can then use NHSN2 analysis tools to generate reports that are displayed on their web browser. NHSN2 addresses data collection from healthcare facilities to permit valid estimation of adverse events among patients or residents and healthcare personnel. Similarly, it provides facilities with risk-adjusted metrics that can be used for inter-facility comparisons and local quality improvement activities. NHSN2 also allows for the opportunity of collaborative research studies with participating facilities that describe the epidemiology of emerging health care-associated infections (HAIs) and pathogens, assess the importance of potential risk factors, further characterize HAI pathogens and their mechanisms of resistance, and evaluate alternative surveillance and prevention strategies. The NHSN2 Agreement ensures compliance with legal requirements – including state or federal laws, regulations, or other requirements – for mandatory reporting of facility-specific adverse event, prevention practice adherence, and other public health data. NHSN2 enables healthcare facilities to report data to the Centers for Medicare & Medicaid Services (CMS) of the U.S. Department of Health and Human Services (DHHS) in fulfillment of CMS's quality measurement reporting requirements for those data. Considering the Coronavirus Disease (COVID-19) Pandemic, CDC created the capability for COVID-19 surveillance in NHSN2, enabling data collection reported by Long-Term Care Facilities (LTCFs) and Outpatient Dialysis Facilities. This data is reported through different pathways within the NHSN2 COVID-19 Modules for LTCFs and Outpatient Dialysis Facilities.	

Save

12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The type of information the NHSN2 system collects is described below: Patients: Patient identification number (may be a medical record number), gender and date of birth. For some patients, birth weight is required. Healthcare workers: Healthcare worker identification number, gender, date of birth, work location, and occupation. Facilities: Facility name, address, county, city, state , zip code, telephone number, identifying number (i.e., CMS provider number and/or American Hospital Association identification number and/or Veterans Administration station code), type, ownership category, affiliation with a medical school (y/n), and bed-size characteristics. Users: Name, address (if different from facility), telephone number, and email address. Optional information that may be reported to NHSN2: Patients: Social security number, secondary identification number, name, ethnicity, and race. Healthcare workers: Name, address, work and home phone numbers, email address, born in United States (y/n), ethnicity, race, and date of employment. Users: Fax number, pager number, and title. NHSN2 external users are authenticated through CDC Secure Access Management System (SAMS), which is covered by a separate Privacy Impact Assessment (PIA). NHSN2 internal users access the system via Active Directory (AD) which is a separate system covered by its own PIA.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	NHSN2 data is used by CDC for improving and tracking public health; by CMS for public reporting, payment, and regulatory programs; by Facilities, Systems, and Collaboratives for improving care; and by States and local health departments and Hospital Associations for public health safety reporting. The data is used to provide state and local health departments with information that identifies the facilities in their state that participate in NHSN2 and to provide to state and local health departments, at their request, facility-specific, NHSN2 data for surveillance, prevention, or mandatory public reporting. Any U.S. healthcare institution including hospitals, outpatient centers, and Long-Term Care Facilities (LTCF) may enroll in NHSN2 provided they have access to the Internet. The NHSN2 Registration server provides healthcare administrators with a way to register their facility in NHSN2. After registering their facility, they will be given instructions on how to get a digital certificate and begin using the main NHSN2 application. This registration application also provides a way for users to accept the NHSN2 Rules of Behavior before accessing the main NHSN2 application. NHSN2 external users are authenticated through CDC Secure Access Management System (SAMS), which is covered by a separate PIA. NHSN2 internal users access the system via Active Directory (AD) which is a separate system covered by its own PIA.

Save

14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No
15	Indicate the type of PII that the system will collect or maintain.	☒ Social Security Number ☒ Date of Birth ☒ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☒ Medical Records Number ☒ Medical Notes ☐ Financial Account Info ☒ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☐ Military Status ☒ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Birth weight Ethnicity and Race Work Identification Number Titles Gender
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☒ Employees ☒ Public Citizens ☒ Business Partners/Contacts (Federal, state, local agencies) ☒ Vendors/Suppliers/Contractors ☒ Patients Other
17	How many individuals' PII is in the system?	1,000,000 or more
18	For what primary purpose is the PII used?	Data from NHSN2 is used for tracking of healthcare-associated infections, antibiotic use and resistance, and surveillance of COVID-19.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Data from NHSN2 is also used as a guide for infection prevention activities that protect patients.
20	Describe the function of the SSN.	SSNs are vital to the overall operation of NHSN2 because hospitals whose data is entered into NHSN2 may use NHSN2 to track a patient by SSN. Also state public health officials who have been granted access to the data in their state by their constituent hospitals may require access to patient SSNs. The state of Pennsylvania for example requires by law the reporting of Healthcare Associated Infections using NHSN2 and as part of the state mandate requires the records to be identified by SSNs. This allows Pennsylvania to download data from NHSN2 about patients in their state and link that data to payment information.
20a	Cite the **legal authority** to use the SSN.	E.O. 9397, November 22, 1943 (as Amended by E.O. 13478, 18 November 2008)

Save

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)). 5 U.S.C. 301, 40 U.S.C. 486(c).
22	Are records on the system retrieved by one or more PII data elements?	(•) Yes ( ) No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: 09-20-0136: Epidemiologic Studies and Surveilla Published: 09-90-2001: Records Used for Surveillance and S Published: ☐ In Progress
23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax ☐ Email ☒ Online ☐ Other Government Sources ☒ Within the OPDIV ☐ Other HHS OPDIV ☒ State/Local/Tribal ☐ Foreign ☒ Other Federal Entities ☐ Other Non-Government Sources ☒ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☐ Private Sector ☒ Other
23a	Identify the OMB information collection approval number and expiration date.	OMB No. 0920-0666, expiration Date: 2023-12-31
24	Is the PII shared with other organizations?	(•) Yes ( ) No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	☒ Within HHS: CMS for required COVID-19 reporting and with HHS for ☒ Other Federal Agency/Agencies: Federal Emergency Management Agency (FEMA), Administration for ☒ State or Local Agency/Agencies: Select Healthcare facilities in the U.S. ☒ Private Sector: Some corporate healthcare entities and quality improvement

Save

24b	Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Information and the NHSN Data Use Agreement document can be found at http://www.cdc.gov/hai/surveillance/DUA-announcment.html. Each state or local jurisdiction has requested access to different data—you can read each state's specifics by clicking on the state at http://www.cdc.gov/HAI/state-based/index.html. Each facility can only see it's own data. Health Departments (HD) with NHSN DUAs: Chicago Department of Public Health Harris County Health Department Houston Health Department Los Angeles County Department of Public Health Maricopa County Department of Public Health (Phoenix, AZ) New York City DOH & Mental Hygiene Southern Nevada Health District San Diego (County of San Diego Health & Human Services Agency) Orange County Health Department Arizona Department of Health Services Florida Department of Health Idaho Department of Health and Welfare Indiana State Department of Health Kansas Department of Health and Environment Kentucky Department of Public Health Louisiana Department of Health, Infectious Disease Epidemiology Section Minnesota Department of Health ("MDH") Montana Department of Public Health and Human Services Nevada Division of Public and Behavioral Health New York State Department of Health North Dakota Department of Health Ohio Department of Health South Dakota Department of Health Texas Department of State Health Services(TXDSHS) Vermont Department of Health Washington State Dept of Health (Territory) Guam Department of Public Health and Social Services
24c	Describe the procedures for accounting for disclosures	It is the responsibility of the facility and Electronic Health Record (EHR) vendor to notify patients of any data collected on their behalf. Requests from patients for data submitted to NHSN would be tracked by established processes that are specific to that healthcare facility.
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	N/A; data in NHSN2 is not collected directly from the individual but rather provided from the facilities. It is the responsibility of the facility and Electronic Health Record (EHR) vendor to notify patients of any data collected on their behalf.
26	Is the submission of PII by individuals voluntary or mandatory?	(•) Voluntary ( ) Mandatory
27	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.	N/A; because facilities submit data on behalf of patients. Patients do not submit data directly into NHSN2, but rather NHSN users (facilities) do so on their behalf.

Save

28	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.	Facilities that participate in NHSN2 are responsible for letting individuals know if their PII is being used and as such any concerns regarding this should be directed to the facility.	
29	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.	Facilities that participate in NHSN2 are responsible for letting individuals know if their PII is being used and as such any concerns regarding this should be directed to the facility.	
30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	No umbrella process is in place to ensure the accuracy of the PII contained in the system. Facilities participating in NHSN2 are responsible for the submission and verification of PII in NHSN2.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Users will have access to the PII in the system for Epidemiologic Analysis.
		☒ Administrators	Administrators will have access to the PII in the system for data management
		☒ Developers	Developers will have access to the PII in the system for NHSN2 Development
		☒ Contractors	Direct Contractors with Personal Identity Verification (PIV) cards need
		☒ Others	Epidemiologic Analysis by approved CDC staff and guest researchers.
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All users must be approved by the Business Steward based on their role, duties and responsibilities prior to gaining access to the data. Role Based Access Control (RBAC) is utilized. The roles are predefined and users are assigned those roles as appropriate.	
33	Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	The least privilege model is utilized to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	
34	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 CDC personnel are required to complete annual Security and Privacy Awareness training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Users are required to acknowledge Rules of Behavior attesting to their understanding of the privacy requirements.	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	◉ Yes ○ No	

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	CDC Records Control Policy applies. Records are retained and disposed of in accordance with the CDC Records Control Schedule for NHSN2 records. Records are retained for various periods of time depending upon how useful they are considered to be, in accordance with NHSN2 policy. Some records of users may be maintained indefinitely. Disposal methods include burning or shredding hard copy and erasing computer tapes and disks. NHSN2 record schedule adhere to N1-442-09-001, item 1
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, annual system privacy impact assessments; and mandatory annual security & privacy awareness training. Technical controls include application level role based access controls; encryption of PII at rest and in transit; standard baseline configurations for IT assets; server audit and accountability measures; and continuous monitoring of system resources to identify vulnerabilities and ensure adherence to organizationally defined minimum security requirements. In addition, the system is protected by residing within SAMS and requires each user to have CDC-approved identity proofing in order to access the system. Physical controls surrounding the system's data centers include gated campuses with 24-hour security guards to enforce access restriction; key card access to campus buildings; and access control lists further limiting physical access to sensitive areas such as the data centers.

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

	Reviewer Questions	Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	○ Yes ◉ No
Reviewer Notes	See email re concerns: Qs 4, 12-13, 24-25, 27, & 39-43. Please address concerns.	
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	○ Yes ○ No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	○ Yes ○ No
Reviewer Notes		
4	Does the PIA appropriately describe the PII quality and integrity of the data?	○ Yes ○ No
Reviewer Notes		

Save

	Reviewer Questions	Answer
5	Is this a candidate for PII minimization?	○ Yes ○ No
Reviewer Notes		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	◉ Yes ○ No
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	○ Yes ◉ No
Reviewer Notes	See email for concerns re Qs 24-25 &27	
8	Does the PIA raise any concerns about the security of the PII?	○ Yes ○ No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	○ Yes ○ No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	○ Yes ○ No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	○ Yes ○ No
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	○ Yes ○ No
Reviewer Notes		

General Comments	SOP/CPO signature of this version of the revised PIA is ONLY for the purpose of approval of the eRAP associated with this system; not the ATO. It is expected that the program will continue to expediently collaborate with the CDC Privacy Team to gain approval of the final PTA/PIA using the ARCHER GRC tool Once that PIA is finalized in ARCHER (including HHS approval), it will be used for the ATO.

OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2023.12.05 16:17:46 -05'00'	HHS Senior Agency Official for Privacy	