Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft | Form Number F-90191 | Form Date 1/3/2023 8:42:36 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6798149-611197
2a	Name:	National Healthcare Safety Network (NHSN)
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.	Operations and Maintenance
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: Deputy 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
8a	Date of Security Authorization	Mar 10, 2023

Save

11	Describe the purpose of the system.	The major purpose of the National Health Safety Network (NHSN) 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. NHSN provides analysis tools that generate reports using the aggregated data (reports about infection rates, national and local comparisons, etc.). Participating NHSN 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 NHSN analysis tools to generate reports that are displayed on their web browser. NHSN 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. NHSN 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 NHSN 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. NHSN 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 NHSN, enabling data collection reported by Long-Term Care Facilities (LTCFs) and Outpatient Dialysis Facilities. This data is reported through different pathways within the NHSN COVID-19 Modules for LTCFs and Outpatient Dialysis Facilities.
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 NHSN system collects is described below: Patients: Patient identification number (may be a medical record number), gender and date of birth. For some patients,
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The National Healthcare Safety Network (NHSN) system exists to provide state and local health departments with information that identifies the facilities in their state that participate in
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No

Save

15	Indicate the type of PII that the system will collect or maintain.	☒ Social Security Number ☒ Name ☐ Driver's License Number ☐ Mother's Maiden Name ☒ E-Mail Address ☒ Phone Numbers ☒ Medical Notes ☒ Certificates ☐ Education Records ☐ Military Status ☐ Foreign Activities ☐ Taxpayer ID Birth weight Ethnicity and Race Work Identification Number Titles Gender ☒ Date of Birth ☐ Photographic Identifiers ☐ Biometric Identifiers ☐ Vehicle Identifiers ☒ Mailing Address ☒ Medical Records Number ☐ Financial Account Info ☐ Legal Documents ☐ Device Identifiers ☒ Employment Status ☐ Passport Number
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 NHSN 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 NHSN 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 NHSN because hospitals whose data is entered into NHSN may use NHSN 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 NHSN and as part of the state mandate requires the records to be identified by SSNs. This allows Pennsylvania to download data from NHSN 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 Surveillance of Disease Problems. HHS/CDC. Published: 09-90-2001: Records Used for Surveillance and Study of Epidemics, Preventable Diseases and Problems 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	

Save

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 COVID-19 pandemic response ☒ Other Federal Agency/Agencies Federal Emergency Management Agency (FEMA), Administration for Strategic Preparedness and Response (ASPR), and the White House Coronavirus Task Force for pandemic response ☒ State or Local Agency/Agencies Select Healthcare facilities in the U.S. These facilities may track a patient using SSN. Specifically Pennsylvania requires by law the reporting of healthcare associated infections using NHSN and as part of the state mandate requires the records to be identified by SSNs. State, local, and territorial health departments access PII for purposes of surveillance and response. ☒ Private Sector some corporate healthcare entities and quality improvement organizations have access to PII for purposes of surveillance and prevention with the consent from individual facilities

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	The NHSN User Support Helpdesk currently tracks for accounting for disclosures via management of an organized email folder system.
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.	NHSN is a public health surveillance system and does not require obtaining consent from individuals whose data are submitted and stored in the system. When facilities agree to the NHSN Agreement to Participate and Consent upon enrollment in NHSN, they are made aware of the purposes of NHSN and how the data reported to NHSN may and may not be used, including PII.
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.	There is no option to object to the information collection because NHSN is a public health surveillance system that requires healthcare facilities to submit patient data for public health surveillance.

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 NHSN 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 NHSN 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 NHSN are responsible for the submission and verification of PII in NHSN.	
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 purposes.
		☒ Developers	Developers will have access to the PII in the system for NHSN Development and Maintenance.
		☒ Contractors	Direct Contractors with Personal Identity Verification (PIV) cards need access to perform Epidemiologic Analysis.
		☒ 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	
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 NHSN records. Records are retained for various periods of time depending upon how useful they are considered to be, in accordance with NHSN policy. Some records of users may be maintained indefinitely. Disposal methods include burning or shredding hard copy and erasing computer tapes and disks. NHSN 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.	

Save

General Comments	Q10: In response the COVID-19 pandemic, the National Healthcare Safety Network (NHSN) augmented the existing NHSN system to monitor and analyze the capacity of the domestic healthcare system so that federal, state, and local officials can adjust their response efforts. This augmentation encompassed the distinct COVID-19 reporting modules including a hospital capacity and patient impact COVID-19 module for hospitals, a long-term care facility (LTCF) COVID-19 module, an outpatient dialysis module, and collection of Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) point-of-care antigen test data from long-term care facilities. On May 8, 2020, the Centers for Medicare and Medicaid Services (CMS) published an Interim Final Rule with Comment Period to mandate that all approximately 15,600 CMS-certified nursing homes report standard COVID-19 data to NHSN through the LTCF COVID-19 module. As part of this rule, CMS publicly reports facility-level nursing home data. Facilities began to submit data to this module on May 17, 2020 and must submit data through NHSN at least once every seven days. It should be noted that reporting into the hospital capacity and patient impact COVID-19 module began in March of 2020 and ended on July 15, 2020. Reporting into the dialysis module began in November of 2020. SARS-CoV-2 point-of-care antigen test data from long-term care facilities is reported to NHSN and then transmitted via HL7 Clinical Documentation Architecture to the Association of Public Health Laboratories' Informatics Messaging Services (AIMS) platform. The data is then provided to State Health Departments and HHS. In addition to NHSN's response to the pandemic, NHSN's new Neonatal Component is expected to launch during the winter of 2020/2021. This component will focus on premature neonates and the healthcare-associated events that occur as a result of their prematurity. This component will be released with one module, which includes Late Onset-Sepsis and Meningitis, which are common complications of extreme prematurity. There is no manual entry available to users for the new neonatal component. Both numerator and denominator data will be imported into the Clinical Document Architecture (CDA) via electronic data transfer. This will allow users to obtain data submitted via CDA and focus on prevention activities within their respective hospitals or facilities. All data collected in these modules and in the POC initiative fall under the personally identifiable information (PII) previously specified in the hospital acquired infection (HAI) data collected by NHSN.
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2023.01.19 11:46:41 -05'00'