Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-37361 | Form Date: 1/22/2020 10:17:16 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-4490559-562460
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: Branch Chief POC Name: Daniel Pollock POC Organization: NCEZID/DHQP POC Email: Dap1@cdc.gov POC Phone: 404-639-4237
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	April 2, 2020 ☐ Not Applicable

Save

11	Describe the purpose of the system.	NHSN allows participating healthcare facilities to enter data associated with healthcare safety events, such as surgical site infections, antimicrobial 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.
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.)	NHSN is a voluntary surveillance system. The system requires reporting of the following information: 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 NHSN: 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. NHSN users are authenticated through CDC Secure Access Management System (SAMS), which is covered by a separate PIA.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	NHSN is the nation's most comprehensive medical event tracking system used by more than 22,000 U.S. healthcare facilities in all 50 states, Washington, D.C., and Puerto Rico. Data from NHSN is used for tracking of healthcare-associated infections and guides infection prevention activities that protect patients. CMS and other payers use these data to determine incentives for performance and members of the public may use the data to select among available providers. Each of these parties relies on the completeness and accuracy of the data. NHSN allows participating healthcare facilities to enter data associated with healthcare safety events, such as surgical site infections, antimicrobial 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). NHSN also provides links to best practices, guidelines, and lessons learned. Participating NHSN healthcare facilities can access web-based screens that allow them to enter data associated with healthcare safety events. Any U.S. healthcare institution including hospitals, outpatient centers, and long-term care facilities may enroll in NHSN provided they have access to the Internet. Along with NHSN there is an NHSN Registration server that provides healthcare administrators with a way to register their facility in NHSN without having a digital certificate. After registering their facility they will be given instructions on how to get a digital certificate and begin using the main NHSN application. This registration application also provides a way for users to accept the NHSN Rules of Behavior before accessing the main NHSN application. NHSN is a voluntary surveillance system. The system requires reporting of the following information: 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 NHSN: 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. NHSN users are authenticated through CDC Secure Access Management System (SAMS), which is covered by a separate 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 Race Titles Gender Work Identification Number Certificates
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.
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.

Save

20a	Cite the **legal authority** to use the SSN.	E.O. 9397, November 22, 1943 (as Amended by E.O. 13478, 18 November 2008)
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)).
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: 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: 01/31/2021
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 ☐ Other Federal Agency/Agencies ☒ State or Local Agency/Agencies Select Healthcare facilities in the U.S. These facilities may track a patient using SSN. Specifically PA 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. ☐ Private Sector
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. So far we have agreements with AZ, KY, LA, MN, and NY. Each state 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.
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.
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 Antimicrobial Resistance surveillance.
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.

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Epidemiologic Analysis
		☒ Administrators	Database Management
		☐ Developers	
		☒ Contractors	Direct Contractors 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 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 a 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	
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, N1-442-09-1, item 1 () NHSN adheres to GRS 20.2a.4, 20.2d, 20.6 and RCS B-321, 2.	

Save

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.

General Comments	
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2020.02.26 11:06:21 -05'00'