U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT

Name of Application/System:	Web NEISS
Office/Directorate:	EXHR/EPI/EPDS
Date:	04/15/2021

A. CONTACT INFORMATION

Person completing PIA: (Name, title, organization and ext.)	**Tom Schroeder, Division Director, EPDS, x7431**
System Owner: (Name, title, organization and ext.)	Tom Schroeder, Division Director, EPDS, x7431
System Manager/Technical POC: (Name, title, organization and ext.)	Jason Jen, IT Specialist, ITSD, x7724

B. APPROVING OFFICIALS

Tom Schroeder Digitally signed by Tom Schroeder
DN: cn=Tom Schroeder, o, ou=U.S. Consumer Product Safety Commission, email=tschroeder@cpsc.gov, c=US
Date: 2021.04.15 09:47:26 -04'00'

System Owner Date

Senteria Jones Digitally signed by Senteria Jones
Date: 2021.06.01 10:30:03 -04'00'

Privacy Officer Date

PATRICK MANLEY Digitally signed by PATRICK MANLEY
Date: 2021.06.02 15:08:56 -04'00'

Chief Information Security Officer (CISO) Date

ABIOYE MOSHEIM Digitally signed by ABIOYE MOSHEIM
Date: 2021.05.26 07:08:32 -04'00'

Asst. General Counsel for FOIA, Records and Privacy Date

JAMES ROLFES Digitally signed by JAMES ROLFES
Date: 2021.06.03 15:49:48 -04'00'

Senior Agency Official for Privacy (SAOP) Date

C. SYSTEM OF RECORDS NOTICE

1. Will the system or application maintain records that contain information about individuals? Yes ☑ No □

2. Will the system or application allow records to be retrieved by a personal identifier*? Yes □ No ☑

If the answer to both 1 and 2 above is "Yes," then the system requires a System of Records Notice (SORN).

* *A personal identifier might include an individual's name, address, email address, telephone number, social security number, photograph, biometric information, or any other unique identifier that can be linked to an individual.*

D. PRIVACY ASSESSMENT

1. Will the system or application be used to collect, store, or transmit personally identifiable information (PII)*?
   Yes ☑ No □ (If there is **NO** information collected, stored, or transmitted that is identifiable to the individual, the remainder of this PIA does not have to be completed.)

** Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. (e.g. Social Security numbers, Passport numbers, etc.)*	
2. Generally describe the type of information that will be collected, stored, or transmitted.	NEISS contains information on product-related injuries treated in hospital emergency rooms (ER). Records include data such as the treatment date, product, age, sex, race and ethnicity, diagnosis, injured body part, disposition, and a brief narrative describing the nature of the injury and how it happened. Some records contain date of birth. Some records contain more specific information about
3. What categories of individuals are covered in the system? (public, employees, contractors)	Public
E. SYSTEM DATA	
4. Is the PII collected verified for accuracy? Why or why not?	NEISS hospitals are evaluated at least annually. An evaluation consists of independently coding a set of records that the NEISS coder has already entered and verifying the accuracy of those records. Any inaccuracy is discussed with the NEISS coders and corrected. When a case is assigned for a follow-back interview, the victim is contacted and has an opportunity to verify and/or correct any inaccurate information.
5. Is the PII current? How is this determined?	The information being captured is a record of an ER visit and is generally not subject to change and is considered current.
6. Who will be responsible for protecting the privacy of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability?	IT administrators and EPDS management. Victim contact information can only be accessed by EPDS staff and those involved in conducting follow-back interviews. Victim contact information is deleted from the database automatically, 30 days after it is entered. Victim contact information is maintained by
7. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?	Victim contact information is maintained until the follow-back interview is completed or terminated. When a case is assigned for a follow-back interview, the victim is contacted and has an opportunity to verify and/or correct any inaccurate PII.
8. Is the source of the information from the individual or is it taken from another source? If not directly from individual, then what other source?	No information is gathered directly from the public. The information is abstracted by a contractor from medical records in the hospital.
F. MAINTENANCE AND ADMINISTRATIVE CONTROLS	

9. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?	Individuals do not have an opportunity to decline for the information in the basic NEISS record to be collected, but they may decline to participate in any follow-back interview. Hospitals may also decline to provide victim contact information for follow-back interviews.
10. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII.	NEISS data is interconnected with several systems including CPSRMS and IFS. NEISS data that involve deaths are interconnected to CPSRMS for use by CPSC staff. A limited set of NEISS data with Victim ID can be retrieved through IFS for follow-back investigations.
11. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?	EXIT contractors are involved in programming and maintaining the system. Contractors are also involved in the collection of the data. CPSC has contracts with both the hospitals providing the data and in some cases with third party coders (usually hospital employees) who do the actual coding of the data. Each contract includes the
12. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?	NEISS records are retained indefinitely. Victim contact information (Name, Address, Phone Number) is deleted from the database automatically, 30 days after it is entered.
13. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)?	NEISS records are kept indefinitely. Victim ID is deleted from the database automatically, 30 days after it is entered.
14. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?	No.
G. ACCESS TO DATA	
15. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).	Victim contact information can only be accessed by EPDS staff and those involved in conducting follow-back interviews. The basic NEISS data may be retrieved for analysis by most CPSC staff, including technical staff, IT staff, and contractors. NEISS data is also made available to the public with "purged narratives" (all information that might identify an individual, hospital, location, or

16. What controls are in place to prevent unauthorized access to the data?	Victim contact information can only be accessed by EPDS staff and those involved in conducting follow-back interviews. EPDS management and EXIT review who is given access to the data. The basic NEISS data may be retrieved for analysis by most CPSC staff, including technical staff, IT staff, and contractors.
17. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access?	CPSC and EPDS policies and procedures for handling PII apply. All CPSC staff must complete annual mandatory privacy and security training. EPDS and contract staff must also receive additional information security training (live or via an e-mailed PowerPoint in alternate years) and affirm that they have read the CPSC directives relating to information security. Relevant training
18. Is access to the PII being monitored, tracked, or recorded?	No.
19. For CPSC support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval?	CPSC has contracts with both the hospitals providing the data and in some cases with third party coders (usually hospital employees) who do the actual coding of the data. Each contract includes the Privacy Act clause. EXIT management determines access for IT contractors.
20. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared?	None.
21. What CPSC personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)?	All
22. Will any of the personally identifiable information be accessed remotely or physically removed?	Yes. CPSC staff and contractors that tele-work have access to the data retrieval systems. Victim contact information is transmitted securely through a data transmittal application approved by CPSC IT staff to the contractors conducting follow-back interviews.