

**U.S. Consumer Product Safety Commission
PRIVACY IMPACT ASSESSMENT**

| | |
|----------------------------|-----------|
| Name of Project: | EP Review |
| Office/Directorate: | EPDS |

A. CONTACT INFORMATION

| | |
|-----------------------------------------------------------------------|--------------------------------------------------------|
| Person completing PIA: (Name, title, organization and ext.) | Jean Mah, Branch Chief, EPDSS, x7659 |
| System Owner: (Name, title, organization and ext.) | Thomas Schroeder, Director, EPDS, x7431 |
| System Manager: (Name, title, organization and ext.) | Nidhu Nijhawan, Supervisory IT Specialist, EXIT, x6812 |

| B. APPROVING OFFICIALS | Signature | Approve | Disapprove | Date |
|-------------------------------|------------------|----------------|-------------------|-------------|
|-------------------------------|------------------|----------------|-------------------|-------------|

| | | | | |
|------------------------------------------------------------------------------------------------------------------------|----------------------------|----------|--|---------|
| System Owner Thomas Schroeder, Director | Thomas Schroeder, Director | X | | 2/16/18 |
| Privacy Advocate Bobby Sanderson, EXIT | Bobby Sanderson, ISSO | | | |
| Chief Information Security Officer Patrick Manley, EXIT | Patrick Manley, CISO | X | | 4/20/18 |
| Senior Agency Official for Privacy James Rolfes, EXIT System of Record? _____ Yes <u> X </u> No | James Rolfes, CIO | X | | 4/30/18 |
| Reviewing Official: James Rolfes, EXIT | James Rolfes, CIO | X | | 4/30/18 |

C. SYSTEM APPLICATION/GENERAL INFORMATION

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. Does this system contain any personal information about individuals? (If there is NO information collected, maintained, or used that is identifiable to the individual, the remainder of PIA does not have to be completed.) | Yes |
| 2. Is this an electronic system? | Yes |

D. DATA IN THE SYSTEM

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. What categories of individuals are covered in the system? (public, employees, contractors) | Public |
| 2. Generally describe what data/information will be collected in the system. | NEISS contains information on product-related injuries treated in hospital emergency rooms. Records include data such as the treatment date, product, age, gender, race, 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 the nature of injuries; for example, medications involved in poisonings, whether an injury was work-related, whether an injury was intentional, etc. For a small subset of records we also collect victim ID – name, address and phone number. |
| 3. 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. |
| 4. How will data be checked for completeness? | Completeness of individual records: the program used to enter NEISS records has a number of edits which prevent saving of incomplete records. Completeness of data submitted for a given period: EPDS monitors summary statistics such as percentage of hospitalizations, number of cases per treatment date, etc., which can signal deficiencies in hospital reporting. In addition, on-site evaluation visits are conducted at each participating hospital at least annually. During these visits the evaluator reviews and codes a set of records and compares the result to the records submitted by the hospital coder. This process can detect problems with both completeness and accuracy. |
| 5. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date?) | The information being captured is a record of an ER visit and is generally not subject to change; though in some hospitals there are timing issues that can affect the availability of data to the hospital coder. During evaluation visits the hospital's record flow is reviewed and documented and any problems identified are addressed with the coder and hospital management. |
| 6. Are the data elements described in detail and documented? (If yes, what is the name and location of the document?) | Yes. \\Data_HQ (G:)\USERS\EPDS\READONLY\Library\Database Dictionary\TableFieldsDefined: neismain.xls, neisprod.xls, neiscmt.xls, study09 Child Poison Burn.xls, study04 Firearm.xls, study05 NIOSH Work.xls, study14 CDC Self-Inflicted Violence.xls, study16 ADE.xlsx, study19 CDC Assault.xls, study20 NHTSA MV Non-crash.xls and victim.xls |
| E. ATTRIBUTES OF THE DATA | |
| 1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed? | NEISS is unique in its ability to provide national estimates of product-related injuries. The descriptive data (treatment date, product, age, gender, diagnosis, etc.) that are collected are necessary to identify various populations of interest (i.e. children under five years of age that are poisoned with household chemicals), while the contact information that is provided for some cases allows us to conduct follow-back interviews and obtain more detailed information about the product and circumstances of the injury. |
| 2. For electronic systems, if the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Explain. | PC's used for data entry have encrypted hard disks and user/password authentication. Data are submitted to CPSC over a secure internet connection. Victim contact information is only entered for a few cases and cannot be retrieved once it is entered. At CPSC the data are stored in a database on CPSC's network. Only EPDS staff and those involved in conducting follow-back interviews have access to contact information. Victim contact information is automatically deleted from the database after 30 days. |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>3. How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.</p> | <p>Data are retrieved through the EPIR, EPHQ, and EPReview database applications and through user-written SAS programs. A limited set of NEISS data with Victim ID can be retrieved through IFS for follow-back investigations. Data are retrieved by a combination of Treatment date, a CPSC-assigned hospital identifier and a hospital case number. In lieu of this combination, data may be retrieved by a CPSC-assigned identifier not derived from any values or information on the emergency room data record.</p> |
| <p>4. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information?</p> | <p>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 decline to provide victim contact information for follow-back interviews.</p> |
| <p>F. MAINTENANCE AND ADMINISTRATIVE CONTROLS</p> | |
| <p>1. What are the retention periods of data in this system?</p> | <p>NEISS records are kept indefinitely. Victim ID is deleted from the database automatically, 30 days after it is entered.</p> |
| <p>2. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are procedures documented?</p> | <p>Records in the victim table containing victim ID for assigned cases are deleted automatically from the database 30 days after they are entered. Procedures are documented in the EPDS Information Protection Plan (G:\USERS\EPDS\RDWRITE\security\information protection plan.doc) and in EPDS Internal Operating Procedures to Control Unauthorized Access to Protected Data (G:\USERS\EPDS\RDWRITE\security\DRAFT UPDATE EPDS Internal Operating Procedures.doc).</p> |
| <p>3. For electronic systems, will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.</p> | <p>No</p> |
| <p>4. For electronic systems only, what controls will be used to prevent unauthorized monitoring?</p> | <p>Victim contact information is only retained long enough to complete follow-back interviews and is only accessible to EPDS staff and field staff or contractors conducting the interviews.</p> |
| <p>5. Is this system currently identified as a CPSC system of records? If so, under which notice does the system operate?</p> | <p>No</p> |
| <p>6. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain</p> | <p>N/A</p> <p>No. Most recent SORN applies to current system scope and functions.</p> |
| <p>G. ACCESS TO DATA</p> | |
| <p>1. Who will have access to the data in the system? (e.g., contractors, managers, system administrators, developers, other).</p> | <p>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 and IT staff. NEISS data are also made available to the public with “purged narratives” (all information that might identify an individual, hospital, location, or company is removed) and without identifying information about the source hospital.</p> |
| <p>2. What controls are in place to prevent the misuse of data by those having access? (Please list processes and training materials.)</p> | <p>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 materials and documentation: EPDS Information Protection Plan (G:\USERS\EPDS\RDWRITE\security\information</p> |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>protection plan.doc), EPDS Internal Operating Procedures to Control Unauthorized Access to Protected Data (G:\USERS\EPDS\RDWRITE\security\G:\USERS\EPDS\RDWRITE\security\DRAFT UPDATE EPDS Internal Operating Procedures.doc), NEISS Data Security Plan (G:\USERS\EPDS\RDWRITE\security\NEISS Data Security Plan\NEISS Data Security Plan.pdf), and EPDS Information Security Training (G:\USERS\EPDS\RDWRITE\security\Training\EPDS Information Security Training 2014.pptx).</p> |
| <p>3. Who is responsible for assuring proper use of the data?</p> | <p>IT administrators and EPDS management</p> |
| <p>4. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? Are contractors involved in the collection of the data? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?</p> | <p>Yes – contractors were involved in both the statistical design and in programming the system. Currently maintenance and support is provided by staff within EPDS, with occasional technical assistance by an on-site contractor.</p> <p>Yes – contractors are 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 Privacy Act clause.</p> |
| <p>5. Do other systems share data or have access to the data in the system? If yes, explain. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?</p> | <p>Victim ID is not shared with any other system. Those incidents that are investigated become part of INDP, but those records do not contain any personal identifiers. INDP is managed by the same group as NEISS – IT administrators and EPDS management would be responsible for protecting privacy rights.</p> |
| <p>6. Will other agencies share data or have access to the data in this system? If yes, how will the data be used by the other agency?</p> | <p>No other agencies may directly access the information stored in CPSC's database, but data from the database is extracted and provided to Federal agencies with which we have interagency agreements to conduct NEISS special studies. The data are used for different specific purposes depending upon the study, but generally these agencies use the data similarly to CPSC – to identify the number and nature of injuries and illnesses and develop strategies for reducing the number and severity of these injuries and illnesses. CPSC does not release victim ID to other agencies.</p> |
| <p>7. Will any of the personally identifiable information be accessed remotely or physically removed?</p> | <p>Victim ID is sent to contractors conducting follow-back investigations using a secure data transmittal application approved from CPSC IT staff. The contractor laptops are provided by CPSC and require user/password login. Contractors are instructed to remove Victim ID from the laptops once they have completed or stopped attempts on an interview. CPSC field staff conducting follow-back investigations may access the information remotely. Teleworking EPDS staff may access Victim ID remotely through CPSC network applications. EPDS staff must follow Internal Operating Procedures when removing hard copy materials from the office.</p> |