US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/21/2016

OPDIV:

HRSA

Name:

vx Veterans Integrated System Technology Architecture

PIA Unique Identifier:

P-5765295-616710

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

vx Veterans Integrated System Technology Architecture (vxVistA) , is an applications used to collect, store, retrieve demographic and medical record data on patients treated for Hansen's Disease by the National Hansen's Disease Program. The application is hosted on a Windows 2008R2 server on the internal network within the HRSA OIT GSS boundary.

The National Hansen's Disease Program is the epicenter of Hansen's disease (leprosy) care, research and information in the U.S.
Cares for patients at its facility at the Ochsner Medical Center in Baton Rouge.
Oversees an ambulatory care network with clinics throughout the United States and Puerto Rico and makes referrals for treatment.
Consults with private sector physicians and accepts referrals for patients with Hansen's disease (leprosy)-related complications.
Advances treatment and educates medical professionals about Hansen's disease (leprosy).
Conducts research intramural Hansen's disease (leprosy) biomedical research.

Reaches out to medical professionals with a comprehensive Hansen's disease (leprosy) training program.

The U.S. Government established the predecessor of the National Hansen's Disease (Leprosy) Program, the National Leprosarium in Carville, Louisiana, in 1917. Outpatient clinics were established in 1981.

Describe the type of information the system will collect, maintain (store), or share.

The system is used to collect, store and share information related to patient demographics and Medical Records for in-house staff to included Federal and Direct Contractor to provided service to the patient population served by NHDP.
Demographic data consist of the following elements and are use to identify patients for accuracy in treatment: Name, Date of Birth, Social Security Number (Optional), Mother's Maiden Name (Optional), Mailing Address, Phone Number and E-Mail Address (Optional).
Medical Record data consist of the following elements and are used to document medical history, diagnosis and treatment to better monitor patient care and outcomes: Photographic Identifiers, Medical Records Number, Foreign Activities, Employment Status (Optional), medical notes, medical summaries and correspondence (for example, family to doctor, doctor to doctor, doctor to clinic).

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

Single tier client/server electronic medical records database hosted from a Windows 2008R2 server running a Cache' engine built on the Massachusetts General Hospital Utility Multi-Programming System (MUMPS), currently M code language, for permanent collection of patient data to include PII, Clinical evaluation, treatments and outcomes. Demographic and medical record data are collect to support the National Hansen's Disease Program mission, as defined by public law, to provide accurate patient care for the treatment of Hansen's Disease.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

Photographic Identifiers

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Employment Status

Foreign Activities

medical notes, medical summaries and correspondence

medical history, diagnosis and treatment

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

To assist Internal Staff in the performance of duty to provide accurate patient treatment and care for individuals with Hansen's Disease.

Describe the secondary uses for which the PII will be used.

To provide data for use in facility management, continuing education, Department initiatives, quality assurance activities and research at the National Hansen’s Disease Program, Baton Rouge, Louisiana

Describe the function of the SSN.

Secondary unique identifier for record indexing

Cite the legal authority to use the SSN.

Records indexed by SSN are retrieved in accordance with section 7(a)(2)(B) of the Privacy Act.

Identify legal authorities governing information use and disclosure specific to the system and program.

Section 320 of the Public Health Service Act, as amended (42 U.S.C. 247e), the National Hansen's Disease Program; and section 326 of the Public Health Service Act, as amended (42 U.S.C. 253), Medical Services to Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Service.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-15-0028, PHS Clinical Affiliation Trainee Records

09–15–0007, Patients Medical Record System Public Health Service Hospitals

09-15-0003, Contract Physicians and Consultants

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Government Sources

Other Federal Entities

Identify the OMB information collection approval number and expiration date

Not Required.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Any employee in their official capacity with a need to know to provide accurate patient care for Hansen's Disease

Other Federal Agencies

Need to know for the purpose of assisting the Department's efforts to provide accurate patient care for Hansen's Disease

State or Local Agencies

Need to know for the purpose of assisting the Department's efforts to provide accurate patient care for Hansen's Disease

Describe any agreements in place that authorizes the information sharing or disclosure.

None; All information sharing is done on a need to know bases and requires a signed Consent or Release of Information (ROI) form from each patient at time of request or service.

Describe the procedures for accounting for disclosures.

Copies of written notification (Consent Forms) and Release of Information (ROI) requested are collected at time of service and maintained in the Patient Chart .

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Patients are provided written notification at the time of service as to the data collected, potential use and disclosure.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

Patients are provided the option to opt-out of the collection or use of their PII by refusing service offered by the program.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Notification of major changes are posted to the Federal Register following the SORN process, with Patients provided written notification updates at the time of service as to the data collected, potential use and disclosure. Alternatively Deceased or Patient lost to follow up cannot be notified or have their consent obtained.

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.

Written notification must be sent to Nation Hansen's Disease Program that reasonably identifies the record, specifies the information to be contested, and states the corrective action sought, with supporting justification.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Review of PII data elements contained in the system are conducted during each encounter starting from the first day of service provided and continuing with each subsequent event. During this process clinical staff trained in HIPAA and Privacy rules review and document demographic and medical record information as validate by the patient and staff at time of service; all entries into the system are audited and captured as part of the permanent record. Upon confirmation of errors in the data, a request is submitted with supporting events attached to flag the entry as erroneous; the request is reviewed by a secondary staff member and the necessary action take upon verification. Each staff with access to the system has a unique access/verify code combination along with a signature code required to authenticate and make changes within the system.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Daily data collection as it relates to the mission and patient care

Administrators:

Daily operations as it relates to system performance and availability to end users

Contractors:

Daily data collection as it relates to the mission and patient care - these are direct contractors.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Supervisor initials and approves request for account creation to support job duties, and accounts are created with assigned internal role base controls based on identified job duties and audit logs.

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.

Role base controls are established within the system and assigned during account creation.

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.

Annual department training and review at time of account creation and system access.

Describe training system users receive (above and beyond general security and privacy awareness training).

Verbal and written review of Laws, Regulations and procedures for handling and access system at the time of account creation.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Retention and disposal:Job Number N1-512-92-2

Former Public Health Service Hospitals/Clinics: Destroyed 50 years after date of last treatment, inactive medical records for active duty uniformed service personnel and non-uniformed service personnel.

National Hansen's Disease Program: Retained at facility-not transferred to a Federal Records Center. Destroyed, as appropriate, after 50 years, or when no longer needed for research purposes, as determined by the project leader or principal investigator.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

PII is secured on the system using the following controls:

Safeguards:

Authorized Users: Health care practitioners, and other allied health personnel, medical and allied

health students and administrative personnel for determination of eligibility for care and facility management; qualified research personnel with approved protocol; Public Health Service Commissioned Personnel Operations Division; and Public Health Service Claims Officer.
Physical Safeguards: Magnetic tapes, discs, other computer equipment and other forms of personal data are stored in areas where fire and life safety codes are strictly enforced. All documents are protected during lunch hours and nonworking hours in locked file cabinets in double-locked storage areas.
Procedural Safeguards: A password is required to access the terminal and a data set name controls the release of data only to authorized users. All users of personal information in connection with the performance of their jobs protect information from public view and from unauthorized personnel entering an unsupervised office. Access to records is strictly limited to those staff members trained in accordance with Privacy Act safeguards. These safeguards are in accordance with DHHS Chapter 45-13 and supplementary Chapter PHS.hf: 45-13 of the General Administration Manual, and Part 6 of the DHHS Information Resources Management Manual. The Memorandums of Agreement between the successor organizations and the Public Health Service require the successor organizations to comply with the Privacy Act. Public Health Service and HHS guidelines have been provided to each successor organization.