US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/17/2017

OPDIV:

SAMHSA

Name:

Buprenorphine Waiver Notification System (BWNS)

PIA Unique Identifier:

P-6314988-687987

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

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

Describe the purpose of the system.

The BWNS uses a web-based application form to collect information from physicians who wish to participate in the DATA Waiver program. The Buprenorphine Waiver Management System (BWNS) allows physicians to enter notifications of their intent to prescribe and/or dispense buprenorphine, a DEA designated Schedule III narcotic, for the treatment of opioid dependency. The BWNS consists of both web-based forms for data entry, and a database-driven work flow system that is used to verify the eligibility of applicants to participate in the DATA Waiver program. The BWNS also allows the Substance Abuse and Mental Health Services Administration (SAMHSA)/Center for Substance Abuse Treatment (CSAT)/Division of Pharmacologic Therapies (DPT) and their contractor to evaluate physician qualifications according to the terms of the Drug Addiction Treatment Act of 2000, and certify their waivers under the act. The BWNS provides information about physicians with certified waivers who have agreed to be listed in a public locator.

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

The BWNS uses a web-based application form to collect information from physicians who wish to participate in the DATA Waiver program. Physicians enter the system by entering their DEA registration number and their state license number. Other information that participating physicians provide about themselves include their full name, state where licensed, physical address, telephone number, fax number, and email address. SAMHSA and DEA users who are federal employees and the contractor (non-direct staff) also have access to the BWNS database through a web-based form that is accessed by entering their assigned user name, system generated password, and system generated personal identification number (PIN). Access for contractors (all non-Direct) requires the same user name, password and PIN combination as the SAMHSA and DEA staff. The software development team (all non-direct) accesses the BWNS through direct password protected access to the software development environment within the contractors (DSG, Inc.) computer network. User credentials are maintained for system administrators (SAMHSA employees and direct contractors) in BWNS. User credentials are maintained for system administrators (non- direct contractors) in BWNS.

Log Files and Management Data could contain the following: Server User Access Authentication Logs, Server Resource Utilization including Central Processing Unit/Memory/Disk Read Write, Network events, and database user access authentication logs. The system captures non-PII data elements such as: the type of treatment the practitioner intends to provide, the physical setting where they intend to provide care, and the type of addiction medicine training they have received.

SAMHSA, DEA, and the contractor all require system access to review and provide authorization to applying medical practitioners. Upon authorization by SAMHSA, the applying practitioner is provided a new certificate of registration with a business activity code to identify whether the physician is authorized to treat 30, 100, or 275 patients. The BWNS non-direct contractor staff (system administrators and application reviewers) can also access the BWNS through a desktop interface to the BWNS.

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

The BWNS consists of both web-based forms for data entry, and a database-driven work flow system that is used to verify the eligibility of healthcare providers to participate in SAMHSA's Drug Addiction Treatment Act (DATA) Waiver program. To prescribe or dispense buprenorphine, physicians must complete eight hours of required training, and apply for a physician waiver. These waiver applications are forwarded to the DEA, which assigns the physician a special identification number. DEA regulations require this number to be included on all buprenorphine prescriptions for opioid dependency treatment, along with the physician's regular DEA registration number. SAMHSA reviews waiver applications within 45 days of receipt. If approved, physicians receive a letter via email that confirms their waiver and includes their prescribing identification number.

The BWNS uses PHP-based web forms to collect waiver applications from the public. Other web-based BWNS forms used administratively by SAMHSA, DEA, and contractor staff (non-direct) are password protected and used to facilitate the practitioner verification process. All "privileged" users (SAMHSA users with HHS credentials, DEA direct contractors, and non-direct contractor staff) are individually identified in a secured BWNS administrators table that contains the following data elements: username, full name, email address, telephone number, and PIN. These web forms use multifactor authentication (username, password, and PIN) and are only accessible to privileged SAMHSA, DEA, and contractor staff members. The password protected BWNS desktop interface is available to SAMHSA's BWNS contractor who is responsible for the primary management of the practitioner verification process. The desktop application uses multi factor authentication (username, password, and PIN), and is only available to the BWNS application review staff, system software support team members, and system administrators who work for the BWNS contractor.

The system captures non-PII data elements such as: the type of treatment the practitioner intends to provide, the physical setting where they intend to provide care, and the type of addiction medicine training they have received.

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

Yes

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

Name

E-Mail Address

Mailing Address

Phone Numbers

Certificates

State Medical License Number (user credentials)

DEA Medical License Number (user credentials)

DEA registration number, state where licensed, state medical license number, and fax number.

Addiction Medicine Certification date and training location.

User credentials, fields specifying the type of treatment the practitioner intends to provide, in what physical setting they intend to provide care, and the type of addiction medicine training they have received.

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

Employees are SAMHSA application review staff. Business Partners are DEA application review staff. Public citizens are practitioners that apply to the program. Vendors/Contractors include the non-Direct contractor responsible for managing the software system and screening applications from practitioners.

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

PII is used by medical practitioners in order to file paperwork that will allow them to participate in the program. DEA, SAMHSA, and the DATA Waiver contractor make use of the PII to allow them to evaluate qualified physicians administering, dispensing, and prescribing specific FDA approved controlled substances according to the terms of the Drug Addiction Treatment Act of 2000, and certify their waivers under the act. Login credentials (user name and password) are collected to support and administer BWNS. To access the system, administrators enter login credentials.

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

Not Applicable.

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

Authority of the Controlled Substances Act (21 U.S.C. 822 (f))
Drug Addiction Treatment Act of 2000 (DATA 2000)

Narcotic Addict Treatment Act – 1974.

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.

Division of Pharmacologic Therapies, CSAT/SAMHSA System Notice 09-30-0052 1

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

SMA-167 Form Approved: 0930-0234
Date: 07/31/2018

Is the PII shared with other organizations?

Yes

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

Other Federal Agencies

DEA

Private Sector

With active permission from the medical practitioner, location-related PII for the practitioner is shared through two SAMHSA treatment locator websites.

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

Not Applicable.

Describe the procedures for accounting for disclosures.

Not Applicable.

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

The first page of the online BWNS application forms provide a privacy statement and require acceptance of the system policies before continuing. Privileged system users are only given access based upon specific approval by the system owner or the contractors system administrator staff.

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.

No opt-out method is provided since use of this program and system is entirely voluntary for the public, and contractors must provide PII in order to obtain system access."

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

Notification on any significant changes will be displayed through the BWNS web-based forms, and a corresponding email will be sent to each user.

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.

Individual concerns are addressed through a 1-800 phone number, where individuals can call and inquire about their PII and be directed to the web form where they can revise or review their own information.

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

Accuracy - Databases are updated periodically based on the notifications from DEA.
Integrity - Error checking methods and validation procedures during SAMHSA review are typically relied on to ensure the integrity of data that is submitted.
Availability - Regular maintenance and monitoring of the system by system administrators (non-direct contractor staff).
Relevancy - Routine email blasts to the participating practitioners will also reveal undeliverable email addresses.

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

Users:

To update their own information in the system.

Administrators:

Full access to verify data integrity and valdiate information provided by the medical practitioners.

Developers:

(non-Direct contractors) Full access to verify data integrity, and allow for systems development and improvement.

Contractors:

(non-Direct) Manage and maintain the database and provide verification services for information submitted by practitioners.

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

All access is role based and password protected. BWNS requires authentications by remote users (practitioners), SAMHSA users, and DEA users accessing the application via the public Internet. Privileged users first provide a user name and password to authenticate against a database. System users (administrators, developers, contractors, etc.) of the BWNS authenticate to the network via their approved VPN access with Active Directory authentication. The user then browses to the URL and supplies a user name, password, and PIN to access the application.

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 default profile for each user contains all PII. Therefore privileged users have equal access to all PII information. Non-privileged users have access to their own PII information only.

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 DSG Inc. staff receive annual records management and general security and awareness training.

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

Developers and system administrators also have received HHS significant user training and COOP (Continuity of Operations) training .

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.

All records are stored electronically in a secured database. Records are permanent, and remain a part of the BWNS system perpetually under the Persons Required to Keep Records and File Reports, 21 Code of Federal Regulations (CFR) PART 1304.03.

Further assessment will be conducted to propose a schedule for BWNS under the SAMHSA Records Schedule. The data collected, maintained and stored will not be deleted prior to the system being appropriately scheduled with National Archives and Records Administration (NARA).

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

BWNS stores PII for backup and review purposes by SAMHSA and DEA users. The database is stored behind a firewall from all other networks. Access to the management network is restricted to select personnel. All backups and restorations are performed by the operations team to ensure appropriate data is backed up and restored.

Controls are as follows:
Administrative Controls: Include controls which require action on part of human resources. Administrative controls are the process of developing and ensuring compliance with policy and procedures. They tend to be things that employees may do, or must always do, or cannot do. The administrative controls include, but is not limited to, incident handling, controlled maintenance, and access control for transmission medium.

Technical Controls: Include a class of controls in security that are carried out or managed by computer systems. The technical controls include, but is not limited to, continuous monitoring, information system back-up, and telecommunication services, and maintenance tools.

Physical Controls: Include controls implemented to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. The physical facility is usually the building, other structure, or vehicle housing the system and network components. The physical controls include, but is not limited to, media storage, physical access and authorization, and boundary protection.

Identify the publicly-available URL:

http://buprenorphine.samhsa.gov/forms/select-practitioner-type.php

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes