US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/26/2016

OPDIV:

CMS

Name:

Survey and Certification Providing Data Quickly

PIA Unique Identifier:

P-1950131-939882

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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

No

Identify the operator.

Contractor

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.

Long term care nursing home providers must meet certain federal certification requirements in order to participate in Medicare or Medicaid programs. These requirements, which were enacted under the Nursing Home Reform Act, address an array of issues related to the provision of care for nursing home residents including the provision of sufficient staffing.
More specifically, certified nursing home providers are required by law to have sufficient staff available to provide nursing and related services "such that each resident can attain or maintain the highest practicable level of physical, mental, and psychosocial well-being".

Survey and Certification Providing Data Quickly (SC PDQ) provides summarized survey and certification data to the state survey agency and the Center for Medicare & Medicaid Services (CMS) managers. It provides point and click reports on the results of on-site inspections of institutional providers compiled from over one hundred thousand (100,000) surveys or inspections a year in support of the program to determine if all participating providers are adhering to the ‘Conditions of Participation'.

The application provides summarized reports detailing (Provider, Survey & Deficiency) data as key elements to our task of managing and regulating participating providers. SC PDQ is a tool for assisting users in the overall management of the Survey & Certification (S&C) process across the country.

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

Survey and Certification Providing Data Quickly (SC PDQ) imports data provided by the Certification and Survey Provider Enhanced Reporting (CASPER) national database statistical data resources for science and engineering that supports the S&C data collection process. The data dumped from CASPER contains the results of on-site inspections of institutional providers compiled from over one hundred thousand (100,000) surveys or inspections a year. SC PDQ refreshes or reloads data from CASPER on a weekly basis. CASPER data comes from the separately accredited Quality Improvement and Evaluation System (QIES) system. The CASPER data includes information such as facility names, locations, patient enrollment dates, patient discharge dates, and a large amount of answers to different facility survey questions which assist in developing summarized quality of care results. None of the data imported from CASPER contains any personally identifiable information (PII) or protected health information (PHI). The CASPER data is stored temporarily within SC PDQ.

Username, password, email address, and phone number are collected online directly from the end-users during the account registration for SC PDQ. The account registration information contains end-user PII. All user account information is collected by and stored within SC PDQ and is not shared externally with any other systems or user groups. SC PDQ's user community is primarily based in CMS central & regional offices as well as state agency users from across the country. In addition, SC PDQ is also utilized by external federal agencies such as Government Accountability Office (GAO), Office of Inspector General (OIG) and the Department of Justice (DOJ) for auditing purposes. Federal contractors also have access to the system for administrator and developer purposes as per their contracts.

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

SC PDQ is a standalone system (with no direct connection to other systems, and no sub- systems) and is an alternative reporting platform for the aforementioned Survey & Certification data.

Survey and Certification data is imported via a data dump provided by the Certification and Survey Provider Enhanced Reporting (CASPER) database. CASPER data comes from the separately accredited Quality Improvement and Evaluation System (QIES) system. The data contains no personally identifiable information (PII) or protected health information (PHI) and is comprised of results of on-site inspections of institutional providers compiled from over one hundred thousand (100,000) surveys or inspections a year. The CASPER data includes information such as facility names, locations, patient enrollment dates, patient discharge dates, and a large amount of answers to different facility survey questions. The CASPER data is imported and stored for the purpose of assisting in developing summarized quality of care results. The CASPER data is stored temporarily within SC PDQ.

Username, password, email address, and phone number are collected online directly from the end-users during the account registration for SC PDQ. End-users include individuals from CMS' central & regional offices, state agency users from across the country, federal agencies such as Government Accountability Office (GAO), Office of Inspector General (OIG) and the Department of Justice (DOJ) for auditing purposes, and also federal contractors for administrator and developer purposes as per their contracts. User account information contains personally identifiable information (PII) pertaining to the end-users of the system. User account information is collected directly by SC PDQ, and stored temporarily within SC PDQ. User account information is collected for the purpose of vetting users of the system, and then granting and maintaining access to the system. User account information is not shared with any other system or user group.

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

Phone Numbers

Other - Username and Password

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

Employees

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The username, password, email address, name and phone number are the elements required to create a user account within SC PDQ which allows the user to access the application.

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.

Nursing Home Reform Act of 1987 - The Act was part of the 1987 Omnibus Budget Reconciliation Act. Title IV: Medicare, Medicaid, and Other Health-Related Programs, Subtitle C: Nursing Home Reform.

5 U.S.C. 301, Departmental Regulations

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

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable. Direct collection of federal and contractor user account information is exempt

Is the PII shared with other organizations?

No

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

All users registering for new accounts receive a disclaimer stating that their basic personal information (name, email address, phone number, user name, and password) is being collected as part of the account registration process. Users signing into their account also receive a disclaimer and information on how to modify or remove their PII from the system by contacting the Survey and Certification Providing Data Quickly (SC PDQ) help desk.

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.

Collection is necessary for the use of Survey and Certification Providing Data Quickly (SC PDQ) in order to properly identify users and provide authentication to the system. The user can request to have their PII removed by contacting the SC PDQ help desk, however removal from the system may also mean loss of access to the system.

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

Users will be notified via their email address on record, as well as the Survey and Certification Providing Data Quickly (SC PDQ) landing page if any major changes occur to the system regarding the use of their PII.

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.

Users can submit a service request via the SC PDQ site, call, or email the SC PDQ Help Desk for any questions concerning their PII. Administrators will then verify the user's account information and make the appropriate changes to the PII as per the user request. If the administrator determines that PII was inappropriately obtained, used, or disclosed, the administrator will follow established Center for Clinical Standards and Quality (CCSQ) QualityNet (QNet) Incident Response procedures which will involve submitting an incident ticket with the QNet Help Desk and notifying the Information Systems Security Officer (ISSO) for the system amongst other elements of triaging the issue.

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

User account information within SC PDQ is reviewed and audited per CMS Acceptable Risk Safeguard (ARS) standards for maintaining user accounts. A subset of the ARS 2.0 controls focus on PII and ensuring its confidentiality, integrity, and availability. These controls govern items such as audits of accounts by account managers to verify the continued need for the account as well as the accuracy of account information, establishing regulations for the approval or denial of account creations or modifications, regulating assignment of roles, termination of accounts based off of user departure or account inactivity, etc. Account managers are designated within the federal entities, state facilities, and contractor organizations to audit end-user accounts. At minimum, account managers review accounts for compliance every 180 days, and audit all accounts annually. Account managers notify the SC PDQ help desk of user termination for immediate removal of account access.

Administrator modifications to the data are logged and can be attributed specifically to the user doing the modifications via their SC PDQ credentials. If PII is somehow accidentally or intentionally destroyed by an administrator, it can be restored from backup.

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

Administrators:

Administrators have access to validate users and troubleshoot any user account problems. Non-disclosure agreements are in place as well as specific contract language regarding handling of PII.

Developers:

Developers have access due to their contractual requirement to maintain the database which contains PII. Non-disclosure agreements are in place as well as specific contract language regarding handling of PII.

Contractors:

The contractors are comprised of the Administrators and Developers and have access to the PII as outlined within their respective contract responsibilities. Non-disclosure agreements are in place.

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

The SC PDQ program has developed a roles and responsibilities matrix which is included as an appendix to their System Security Plan (SSP). This matrix defines all users groups and the role-based level of access they will be given to the system to meet their contractual requirements. The role-based level of access also determines their ability to access PII within SC PDQ.

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 role-based level of access determines the ability of end-users to access PII within SC PDQ. Account user groups are broken down into standard users, administrators, and developers. “Permissioning” is applied across the different site pages of SC PDQ so that users only have access to the areas of the site they require to complete their contractually obligated duties.

SC PDQ database access is also restricted to the administrator and developer user groups only, and only to support their contractually obligated duties.

In addition to being role-based, access is least privilege, or the minimum amount of access required to complete their contractual requirements. For instance, typical end-users are not assigned the administrator role, because even though they would still have the ability to complete their jobs, they would have access to PII and other information they do not need to see and should not see. Roles are approved by account managers and are applied by the system administrators.

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 system users are required to take the annual CMS Cyber Awareness Challenge Computer Based Training (CBT) as well as the Identifying and Safeguarding Personally Identifiable Information (PII) training endorsed by CMS.

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

Security and Privacy Awareness training is offered through Computer Based Training to all users. Contractors that have elevated levels of access, such as Administrators or Developers, have to take additional role-based training as required within the CMS Acceptable Risk Safeguards (ARS) 2.0 controls for security.

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.

Username, password, email address, and phone number are collected online directly from the end-users during the account registration for SC PDQ. User account information is stored temporarily within SC PDQ per CMS Acceptable Risk Safeguard (ARS) standards for maintaining user accounts.

Survey and Certification data from CASPER is stored in accordance with the National Archives and Records Administration (NARA) approved guidelines in the Center for Clinical Standards and Quality (CCSQ) File Plan and Record Schedule issued by the CCSQ Business Operations Group (BOG). The disposition authority is N1-440-95-1, listed under the "Survey and Certification" category. The data within SC PDQ will always mirror what is in CASPER. Data is stored temporarily for facilities as long as that facility is participating in Medicare or Medicaid programs. If a facility is no longer participating, data is destroyed after certain pre-defined periods of time which are specifically outlined in the CCSQ file plan. The length of time that the data is maintained before destruction will depend on criteria such as facility participation, facility location, and the survey being administered. Per NARA approved record retention schedules:

1. CMS

a) Non-participating Facilities - Cutoff file after termination or denial. Destroy 6 years after cutoff.

(Disposition Authority: N1-440-95-1, Item 9a1)

b) Participating Facilities –

(1) Maintain the Form CMS-1561-(Health Insurance Benefits Agreement) the two most recent certifications and background/support materials - Maintain in an active file for as long as the facility is participating.

(Disposition Authority: N1-440-95-1, Item 9a2a)

(2) Survey report forms and related documents - Cutoff file after completion of survey. Destroy 6 years after cutoff. (Disposition Authority: N1-440-95-1, Item 9a2b)

(3) Survey report forms and related documents pertaining to access hospitals, nursing homes and home health agencies-Cutoff file after removal from the access category and completion of the survey (form 2567). Destroy 4 years after cutoff.

(Disposition Authority: N1-440-95-1, Item 9a2c)

(4) Mammography Facilities Files - Cutoff file upon approval of schedule and transfer to the FRC. Destroy 3 years after cutoff.

(Disposition Authority: N1-440-95-1, Item 9a2d)

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

Survey and Certification Providing Data Quickly (SC PDQ) PII is secured with a variety of security controls as required by FISMA and the CMS Security Program. Operational controls include but are not limited to: contingency plans and annual testing, backups of all files, offsite storage of backup files, physical security including secure buildings with access cards for entry, secure data center requiring additional access permissions for entry, security guards, background checks for all personnel, incident response procedures for timely response to security and privacy incidents, initial security training with refresher courses annually, and annual role based security training for personnel with assigned security roles and responsibilities. Technical controls include but are not limited to user authentication with least privilege authorization, firewalls, Intrusion Detection and Prevention systems (IDS/IPS), hardware configured with the National Institute of Standards and Technology (NIST) security checklists, encrypted communications, hardware configured with a deny all/except approach, auditing, and correlation of audit logs from all systems. Management controls include but are not limited to: Assessment and Authorization(A&A), annual security assessments, monthly management of outstanding corrective action plans, ongoing risk assessments, and automated continuous monitoring.