US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

June 02, 2026

OPDIV:

IHS

Name:

Pharmacy QMS Simplifi

TPWA Unique Identifier:

T-4720869-792632

Is this a new TPWA?

Yes

Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

No

If SORN is not yet published, identify plans to put one in place.

null

Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

No

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

Expiration Date: 1/1/01 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: N/A

Does the third-party Website or application contain Federal Records?

Yes

Describe the specific purpose for the OPDIV use of the third-party Website or application:

The Simplifi quality management system is a third-party, web-based application that provides a secure platform accessible through an internet browser, allowing IHS staff to use it without installing software on their computers.”

Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?

Yes

Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:

The public does not utilize Simplifi. Simplifi is used by IHS staff.

Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?

Yes

How does the public navigate to the third party Website or application from the OPIDIV?

Other...

Please describe how the public navigate to the thirdparty website or application:

N/A the public does not have access

If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to anongovernmental Website?

null

Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?

Yes

Provide a hyperlink to the OPDIV Privacy Policy:

https://www.ihs.gov/privacypolicy/

Is an OPDIV Privacy Notice posted on the third-part website or application?

No

Is PII collected by the OPDIV from the third-party Website or application?

Yes

Will the third-party Website or application make PII available to the OPDIV?

Yes

Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:

The Simplifi quality management system does not collect personally identifiable information. The PII collected through the third-party web-based application is limited to workforce-related information, such as staff names, work email addresses, job titles, training records, and competency evaluations (assessments of staff skills and qualifications). This information is used to support internal Indian Health Service (IHS) functions including quality assurance (QA—processes that ensure standards are met), compliance tracking (monitoring required regulatory activities), workforce management (tracking staff training and qualifications), and inspection readiness (preparing documentation for regulatory review). The system uses this PII to assign and track required tasks, send alerts for overdue training or competencies, document completion of compliance activities, and generate reports. No direct collection of patient PII or public-submitted information is expected through this system.

Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:

The Simplifi quality management system shares limited workforce-related personally identifiable information as necessary to support internal operations and compliance activities. The types of PII that may be shared include staff names, work email addresses, job titles, training records, and competency evaluation results (assessments of staff qualifications). This information is shared only with authorized parties, including Indian Health Service (IHS) supervisors and administrators, designated compliance and quality assurance (QA—processes that ensure standards are met) personnel, and the contracted third-party vendor that hosts and maintains the system.The purpose of sharing this information is to support key functions such as compliance tracking (ensuring required activities are completed), workforce management (monitoring staff training and qualifications), system administration (maintaining and supporting the platform), and inspection readiness (providing documentation for regulatory review). Information sharing is limited to what is necessary to perform these functions and is conducted in accordance with applicable privacy, security, and contractual requirements. No sharing of patient PII or public-submitted information is expected through this system.

If PII is shared, how are the risks of sharing PII mitigated?

The risk of sharing personally identifiable information in the Simplifi quality management system is

Will the PII from the third-party website or application be maintained by the OPDIV?

No

Describe how PII that is used or maintained will be secured:

The personally identifiable information from the Simplifi third-party website application is maintained by IHS. in this case IHS, even though the system is hosted by a vendor.I n practice, this means that workforce-related PII—such as staff names, work contact information, training records, and competency evaluations—is collected and used by IHS for official purposes (such as compliance tracking, quality assurance, and workforce management) and is considered part of IHS records. The third-party vendor stores and processes the data on behalf of IHS, but does not own it.IHS retains responsibility for how the PII is managed, including oversight, retention (how long records are kept), and protection of the data, in accordance with federal privacy and records management requirements.

What other privacy risks exist and how will they be mitigated?

One risk is excessive data collection (collecting more personally identifiable information (PII—information that can identify an individual) than is needed). This is mitigated by data minimization, meaning the system is configured to collect only workforce-related information necessary for compliance, training, and quality assurance (QA—processes that ensure standards are met).Another risk is inappropriate use of data (using informatfill out the attached form ion for purposes other than intended). This is addressed through access controls and user permissions, along with policies that restrict use of PII strictly to official duties such as compliance tracking and staff management.A third risk is data inaccuracy, which could affect staff records or compliance status. This is mitigated by allowing authorized users to review and update records, along with routine audits (periodic checks) to ensure information remains correct and complete.There is also a risk related to third-party handling of data, since the system is vendor-hosted. This is mitigated through contractual requirements, security assessments, and ongoing oversight to ensure the vendor meets federal privacy and security standards.Another concern is data retention risk (keeping information longer than necessary). This is mitigated by following records retention schedules (rules that define how long data must be kept and when it should be deleted).Finally, there is a risk of user error, such as accidental sharing or improper data entry. This is addressed through staff training, clear procedures, and system safeguards (such as prompts or restrictions that prevent improper actions).Together, these measures help ensure that privacy risks are identified, minimized, and managed appropriately while supporting the system’s compliance and quality functions.