

# US Department of Health and Human Services

## Third Party Websites and Applications Privacy Impact Assessment

**Date Signed:**

January 14, 2026

**OPDIV:**

IHS

**Name:**

DT-Tracker Dashboard

**TPWA Unique Identifier:**

T-5547361-684509

**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: null

**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 system centralizes operational information from the IHS Clinic or hospital to improve accuracy, consistency, and visibility throughout the lifecycle of a medical encounter.

DT-Traker is not an Electronic Health Record (EHR) or clinical system. It supports administrative Revenue Cycle Management (RCM) activities by helping staff manage assignments given to the contractor, monitor progress, maintain documentation, and ensure work moves smoothly through established processes to ensure operational reporting needed for client transparency and internal oversight.

Overall, DT-Traker serves as a centralized tool that improves efficiency, standardization, and throughput across DT-Trak's RCM services while maintaining data integrity and controlled access to

sensitive information.

**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:**

DT-Traker is not meant for members of the public, it is for internal IHS use only. If DT-Traker is not used, DT-Trak personnel would revert to manual, paper-based workflows and email-based communication to process and track contractor work assignments, status updates, documentation, and approvals. Information could still be exchanged directly between DT-Trak staff and Indian Health Service (IHS) supervisors or Contracting Officer Representatives using traditional administrative methods.

**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 OPDIV?**

Other...DT Traker is not meant for member of the general public

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

Authorized personnel are provided secure access instructions directly by DT-Trak. IHS supervisors, Contracting Officer Representatives, and designated contractor staff receive an emailed link to DT-Traker along with login credentials specific to their assigned role. These users access the system only through these direct communications; DT-Traker is not publicly accessible.

**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?**

No

**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:**

[www.ihs.gov/privacy-policy](http://www.ihs.gov/privacy-policy)

**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?**

No

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

No

**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:**

IHS supervisors and Contracting Officer Representatives may receive role-based login credentials to access assigned work queues or approval functions within DT-Traker. These credentials allow them to verify contractor work activity and approve items as part of normal operational workflow. No additional PII will be collected or shared by the OPDIV through DT-Traker.

**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:**

PII will not be shared.

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

No PII will be shared.

**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:**

PII within DT-Traker belongs to the IHS clinic or hospital, is not retained outside of the terms of the contract with IHS by the contractor and is protected using the following security practices: Encryption of data in transit and at rest. Role-based access controls limiting user permissions. User authentication using unique credentials. Audit logging to track key system activity. Regular security assessments conducted by the platform provider. Compliance with applicable data protection standards. Secure data backups to prevent loss or corruption. Least-privilege access principles applied to all users. These measures help ensure PII is safeguarded from unauthorized access or disclosure.

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

Mitigation methods include: Role-based access restrictions and periodic permission reviews. User training and workflow validation controls. Secure transmission methods for integrations. Enforced secure connections and remote-access policies. Structured archiving and controlled access to historical data. These safeguards reduce privacy risks and support responsible handling of personal information.