US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

February 06, 2026

OPDIV:

IHS

Name:

Availity Portal Benefit Verification and Claims Processing

TPWA Unique Identifier:

T-7591765-103115

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:

Portal is a secure, web-based platform that facilitates administrative and business transactions between health care providers, health plans, and other authorized entities. The portal is used to support activities such as eligibility and benefits verification, claims status inquiries, prior authorization submissions, provider enrollment, and secure messaging related to health care operations.

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:

Alternative means include use of telecommunication equipment such as telephone calls or facsimile transmission.

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?

An external hyperlink from an HHS Website or Website operated on behalf of HHS

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

Search a URL or hyperlink

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?

No

Provide a hyperlink to the OPDIV Privacy Policy:

https://www.ihs.gov/hipaa/standards/privacy/

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:

Portal may collect and process information necessary to support health care administrative transactions, which may include:
-User account information (e.g., name, business contact information, user credentials)
-Provider and organization identifiers
-Transactional data related to eligibility, claims, or authorizations
-Audit logs and system usage information

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:

Type of information shared is routine use under Treatment, Payment, and Operations, following the below general categorizations:
1. User / Workforce:
User name, email address, business telephone number, user ID / username, organization or provider affiliation, provider National Provider Identifier (NPI), Tax Identification Number (TIN), when required for transactions, Provider or facility name and address.

2. Patient-Related Data (Limited and Transaction-Specific): Patient name, Date of birth, Member or

insurance, identification number, (Note: Patient information is submitted only when required to perform eligibility, claims, or authorization transactions.)

Purpose of sharing the information: PII is shared for the purpose of verifying user identity and access authorization, conducting health care administrative transactions such as: eligibility and benefits verification, claims status inquiries, prior authorization submissions, provider enrollment and credentialing support. Supporting audit, accountability, and operational integrity of health care operations The information is used solely to support payment and operations.

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

Access controls and role-based access and user authentication

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

Yes

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

PII is maintained in the IHS Resource Patient Management System Electronic Health Record System as part of the claim. Information is secure on the IHS server. HIPAA compliant and SOC 2 compliant, incorporating the industry best practice approach to securing data. Data sent to and from Avality network is transmitted using TLS 1.2 encryption in accordance with Federal Information Process Standards (FIPS) 140-2 and the relevant NIST publications.

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

Privacy Risks: Unauthorized Access: Unauthorized individuals gaining access to protected health information (PHI);Data Breaches: Cyberattacks or accidental exposure of PHI; Improper Disposal: Inadequate disposal of physical or electronic records containing PHI; Insider Threats: Employees or contractors mishandling or misusing PHI.

Mitigation Strategies:

Access Controls: Implement strict access controls to ensure only authorized personnel can access PHI. Use role-based access controls (RBAC) to limit access based on job functions; Encryption: Encrypt PHI both in transit and at rest to protect it from unauthorized access; Regular Audits: Conduct regular audits and monitoring of access logs to detect and respond to any unusual activity;Employee Training: Provide ongoing training to employees on privacy policies, data handling procedures, and recognizing phishing attempts; Data Minimization: Collect and retain only the minimum necessary amount of PHI required for the task at hand; Secure Disposal: Ensure proper disposal of PHI by shredding physical documents and securely erasing electronic files; Incident Response Plan: Develop and maintain an incident response plan to quickly address any data breaches or privacy incidents.