US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

IHS

Name:

Inovalon Benefit Verification and Claims Processing

PIA Unique Identifier:

P-7189674-664987

The subject of this PIA is which of the following?

General Support System (GSS)

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.

Agency

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 Inovalon Benefit Verification and Claims Processing system supports Indian Health Service (IHS) revenue cycle operations by enabling Medicare Electronic Data Interchange (EDI), all-payer eligibility verification, electronic claims submission and correction, remittance advice retrieval, and reporting functions. The system allows IHS to verify patient eligibility for Medicare, Medicaid, and other third-party payers; submit and correct claims; manage adjudication and denials; and retrieve remittance advice. Its purpose is to ensure compliance with federal requirements to bill all available third-party resources, streamline claims processing, reduce denials, and maintain operational continuity for reimbursement activities

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

Please revise your response to read "The system processes Personally Identifiable Information (PII) and Protected Health Information (PHI) as defined under HIPAA and the Privacy Act of 1974. Information is transmitted between IHS, Medicare Administrative Contractors, Medicaid agencies, private insurers, and the contractor via secure electronic connections (VPN/SFTP) as required by

IHS security standards.

The system collects and uses personal and healthcare information to:

Identify patients and providers
Verify insurance coverage
Process and pay medical claims
Support billing accuracy and regulatory compliance
Share necessary data with insurers and authorized partners

It handles both personally identifiable information (PII) and medical/billing data. This includes identifiers such as name, date of birth, medical record number (MRN), email address, Medicaid ID, Medicare Beneficiary Identifier (MBI), tribal enrollment identifier, health plan member ID, subscriber and guarantor information, emergency contact details, and employer information.

The system also processes clinical and service-related data, including diagnosis codes (ICD), procedure codes (CPT/HCPCS), dates of service, service location, referral information, prior authorization details, ordering and rendering providers, admission and discharge information, and types of treatment received.

In addition, it maintains claims and insurance information such as denial reasons, payment and adjustment history, primary and secondary insurance carriers, policy and group numbers, coverage effective dates, deductible and copay details, coordination of benefits, claims payment status, explanation of benefits (EOB), and account balances.

System usage data is also collected, including user roles and permissions, audit logs, access timestamps, and system login records."

If the system collects information (i.e. user credentials) about system users/administrators in order to control access or for a similar purpose, please describe the information that is collected about those users/administrators.

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

The Inovalon Benefit Verification and Claims Processing system supports Indian Health Service (IHS) revenue cycle operations by enabling eligibility verification, electronic claims submission and correction, remittance processing, and reporting. It facilitates billing to Medicare, Medicaid, and other third-party payers, helping ensure compliance with federal requirements, improve billing accuracy, reduce claim denials, and maintain efficient reimbursement processes.To perform these functions, the system collects and uses personally identifiable information (PII), clinical data, and billing/insurance information. This includes patient and provider identifiers, medical and service details (such as diagnoses, procedures, and treatment information), and comprehensive claims and coverage data. It also maintains system usage information, including user roles, audit logs, and access records, to support operational oversight and security."

If the system collects information (i.e. user credentials) about system users/administrators in order to control access or for a similar purpose, please describe the information that is collected about those users/administrators.

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

Yes

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

Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Taxpayer ID
Patient Account Number
Medicaid ID , Medicare Beneficiary Identifier (MBI) , Tribal enrollment identifier, Health plan member ID, Insurance subscriber, ID Guarantor information, Emergency contact information, and Employer information
Diagnosis codes (ICD), Procedure codes (CPT/HCPCS), Dates of service, Service location, Referral information, Prior authorization details, Ordering provider, Rendering provider, Admission/discharge details, Type of treatment received, Claim denial reasons, Payment and adjustment history
Primary insurance carrier, Secondary insurance carrier, Policy number, Group number, Coverage effective dates, Deductible and copay information, Coordination of benefits, Claims payment status, Explanation of Benefits (EOB), and Account balance information
User role/permissions, audit logs, access timestamps, user credentials, and system log in records.

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose of PII/PHI in this system is to accurately match a patient to their insurance and medical services so claims can be verified and paid correctly."

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

The secondary uses are about improving the system, preventing mistakes or fraud, and making sure the process works well overall.

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

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 552a, Privacy Act of 1974; 4 U.S.C. 2901, Federal Records Act; 42 U.S.C. 248, Section 321 of the Public Health Service Act, as amended; 42 U.S.C. 254a, Section 327A of the Public Health Service Act, as amended; 25 U.S.C. 13, Snyder Act; 25 U.S.C. 1601 et seq., Indian Health Care Improvement Act; and 2 U.S.C. 2001-2004, Transfer Act of 1954.

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.

09-17-0001 Medical, Health, and Billing Records SystemsSORN history: 75 FR 1625 (1/12/10), *83

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Identify the OMB information collection approval number and expiration date

Written Opt In

Identify the OMB information collection approval number and expiration date

Exempt from an OMB Information Collection Number through Public Law 114-255, the 21st Century Cures Act, Section 2035: Exemption for IHS from the Paperwork Reduction Act requirements.

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.

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of Protected Health Information (PHI) and of the individual's rights and IHS' legal duties with respect to PHI. A copy of the Notice is provided to new patients, patients whose charts are reactivated, and patients who reach legal age. A copy of the notice is given to the patient upon establishing a record or when requested. The staff member providing the notice has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed Acknowledgment of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record. The notices are displayed in the facility as well as on IHS website. IHS employees are notified at the time of hire that their Personally Identifiable Information (PII) will be collected and give consent as it is part of the on-boarding process.

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.

Per the policy provided in the Indian Health Manual Part 2 Chapter 7 Section 22, "Under the HIPAA Privacy Rule, patients have the right to request restriction(s) of the use and/or disclosure of their PHI to carry out treatment; payment and health care operations; inpatient hospital directory; and disclosures to relatives, family members, personal representatives, close friends, health care givers, and any other person involved in the patient's care or payment who is identified by the patient. The IHS is not required to agree to the request. However, a patient still may object to the disclosure of information for the inpatient hospital directory and to relatives, friends, and others involved in patient care under 45 CFR 164.510(b). See Section 2-7.19, "Procedure for the Uses and Disclosures of Protected Health Information for Involvement in the Patient's Care and for Notification Purposes. The initial collection of PII occurs at the various healthcare facilities at the point of registration and is required to determine eligibility for services. All patients at all facilities are provided with a Notice of Privacy Practices. They are also offered Form IHS-810, "Authorization for Use or Disclosure of Protected Health Information". By completing and signing this document, patients may consent to or decline sharing of their protected health information with external entities outside the I/T/U ecosystem through the 4DH and eHealth Exchange.

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

It is IHS policy to provide adequate notice of its uses and disclosures of PHI/PII and of the individual's rights and IHS' legal duties with respect to PHI/PII. The IHS prominently and clearly displays the Notice in every facility. A copy of the Notice is also provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office or other appropriate department provides a copy of the current Notice to the patient. The patient acknowledges receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. An IHS staff member signs and dates the Acknowledgement form and files the signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" into the patient's medical record. No less than every three years, IHS provides notification of the availability of the Notice and how to obtain the Notice. If the Notice is revised by a material change, the revised Notice must be posted in clear and prominent locations in every facility and on its web site, on or after the effective date of the revision. The revised Notice will be posted on the IHS website within the 60 days of a material revision. The revised Notice is also given to all patients who come into a facility after the effective date of the revision and is available upon request on or after the effective date of the revision. Additionally, IHS provides the revised notice to all eligible patients registered in the patient registration system within 60 days of the revision of the Notice. Any individual, whether or not a patient, has the right to request and receive a copy of the Notice at any time, except an inmate. Inmates have no rights to the Notice (45 CFR § 164.520 (a)(3)).

IHS employees are notified at the time of hire that their PII will be collected and give consent as it is part of the on-boarding process.

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.

According to IHS policy all complaints regarding HIPAA Privacy and Privacy Act violations shall be addressed to the Chief Executive Officer or designee. Complaints must be documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Individuals may also file complaints directly to the Secretary, Department of Health and Human Services (HHS).

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

Periodic reviews are performed to make sure personally identifiable information (PII) in the Inovalon Benefit Verification and Claims Processing system remains accurate, available, relevant, and protected. Patient and insurance information, such as name, date of birth, insurance member ID, and claim detail are reviewed during eligibility checks, claims submission, claim corrections, remittance processing, and denial management to ensure the correct information is being used for billing and reimbursement. Authorized billing, revenue cycle, and system support staff verify that records are current and complete before claims are submitted or corrected. Duplicate, outdated, or incorrect information is corrected through normal claims management and account reconciliation processes. Access to records is limited to authorized users, and audit logs help monitor activity and identify errors or improper access. Regular system maintenance, security monitoring, and compliance reviews also help ensure data remains available, protected, and consistent with federal billing and privacy requirements.

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

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

Access to personally identifiable information (PII) within the system is restricted through role-based access controls, formal account management procedures, and supervisory oversight consistent with HHS, IHS, and federal information security requirements. Formal access request must be submitted and approved by superivsors and users must complete required annual privacy and ISSA security awareness training annually. Unique user IDs and authentication mechanisms are in place and overseen by supervisor and Application Coordinators. Access levels are provisioned based on documented business needs. Accounts are disabled promptly upon separation, role change, or contract termination.

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles.

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 personnel with access to the system, including federal employees and contractor staff, are required to complete mandatory privacy and security training to ensure they understand their responsibilities for safeguarding personally identifiable information (PII) and protected health information (PHI). All users must complete annual HHS/IHS Privacy Act and HIPAA training prior to being granted system access and annually thereafter.

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

In addition to mandatory annual security and privacy awareness training, system users receive role-based and system-specific training tailored to the eligibility verification, claims processing, and consent management functions performed within the system. Registration and benefit coordinators receive additional training on consent and health information exchange procedures, including issuance and processing of attestation, opt-out, and opt-back in forms, documentation requirements, and tracking procedures. Supervisors and administrators receive training on role-based access management, least privilege enforcement, audit log review, and account provisioning/deactivation procedures.

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.

The retention and destruction of personally identifiable information (PII) within the system are governed by approved National Archives and Records Administration (NARA) records retention schedules and HHS/IHS records management policy. Records are maintained under NARA General Records Schedule (GRS) 4.1-Records Management Records, where applicable to administrative docuementation. and Indian Health Service Records associated with SORN 09-17-0001Medical, Health, and Billing Records Systems.

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

Personally Identifiable information (PII) in the system is protected through layered administrative, technical, and physical safeguard consistent with HHS, IHS, HIPAA, and the Federal Information Security Management Act requirements. Administrative controls include role-based access approvals, least privilege enforcement, annual privacy and security training, signed Rules of

Behavior, contractual protections, periodic access reviews, and documented incident response procedures. Technical safeguards include unique user IDs, role-based access controls, strong authentication, encryption of data in transit via secure Virtual Private Network Secure File Transfer Protocol, audit logging and monitoring, and session timeout/account lockout mechanisms. Physical protections include secured facilities with controlled access, badge-restricted entry, locked workstations, and secure media destruction in accordance with federal standards.

Identify the publicly-available URL:

https://providercloud.inovalon.com/Auth/?redirect=%2f%3flastForcedProfileUpdate%3d06%252F18%252F2024%252023%253A24%253A22

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?

No

Does the website use web measurement and customization technology?

No

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