

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/03/2025

OPDIV:

CMS

Name:

COMPASS WEB

PIA Unique Identifier:

P-8056478-878050

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?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

Added workflow and functionality for our Task Order 3.

Describe the purpose of the system.

Livanta LLC ("Livanta") is a Medicare Beneficiary and Family Centered Care - Quality Improvement Organization (BFCC-QIO) that contracts with CMS to perform medical record review functions, including quality of care reviews, beneficiary complaint reviews, discharge, and termination of service appeals in various provider settings, medical necessity reviews, and Emergency Medical Treatment and Labor Act (EMTALA) reviews, among others, for which payment is made under Medicare. Livanta is one of two BFCC-QIOs that perform these services in the U.S. and manages case reviews for CMS Regions 2, 3, 5, 7, and 9. Livanta also provides CMS with nationwide claim review services as part of its BFCC-QIO duties. CompassWeb is the internal application/system Livanta uses to support those services. QIOs are authorized under Title XI Part B, Title XVIII, and Sections 1152-1154 of the Social Security Act. The QIO Program is an essential resource in CMS's

effort to improve the quality and efficiency of care for Medicare beneficiaries by expeditiously addressing individual Medicare beneficiary complaints, provider-based notice appeals, violations of the Emergency Medical Treatment and Labor Act (EMTALA), and other Medicare beneficiary concerns outlined within the QIO regulations/law.

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

Livanta uses CompassWeb to collect and maintain the following beneficiary information: Names; Dates of birth; Mailing addresses; Phone numbers; Medical records and notes; Medical records numbers; Legal documents (e.g., powers of attorney); Device identifiers; Employment status; Health Insurance Claim Numbers (HICN); and Medicare Beneficiary Identifier (MBI). The system also collects and maintains information about the entity providing healthcare services, including Names; Mailing addresses; Email addresses; Phone numbers; Fax numbers; National Provider Identifiers (NPI); and Medicare Provider Numbers, as well as pre-decisional and decisional information about the discharge process, the quality of care received, the medical necessity, and coding correctness of services rendered. Quality of Care Reviews, including beneficiary complaint reviews and general quality of care reviews; Beneficiary appeals of denials of hospital admissions, discharge and termination of services (Grijalva, BIPA and Weichardt appeals); Reconsiderations; Medical Necessity Reviews; EMTALA Reviews; Sanctions and/or Sanction Activities; Quality Improvement Initiatives (QIIs); Monitoring Physician Acknowledgement Statement; Person/Patient and Family Engagement including Immediate Advocacy; Pre-Admission/Admission Hospital Issued Notice of Non-coverage (HINN); Short Stay (2 Midnight) Reviews; Higher-Weighted Diagnosis Related Group (HWDRG) Reviews; Readmissions Reviews; Any additional statutory requirements. CompassWeb is used to record and share medical record review data and case notes from Livanta authorized employees and approved subcontractors. Additionally, CompassWeb is used to compose, send, and store determination letters to providers and beneficiaries and run reports on statistical and other management data. The CompassWeb system is a Livanta-maintained, standalone system. Livanta authorized employees and approved subcontractors are not direct contractors of CMS and do not have HHS credentials. However, the system stores the required user identities and credentials, e.g., username and password, for its authorized Livanta users. No CMS employees access this system.

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

As a Beneficiary and Family Centered Care-Quality Improvement Organization (BFCC-QIO), Livanta conducts various Medicare beneficiary medical reviews. These include but are not limited to, quality-of-care reviews (encompassing beneficiary complaint reviews and general quality of care reviews), beneficiary discharge and termination of service appeals, medical necessity reviews, reviews of Emergency Medical Treatment and Labor Act (EMTALA) services, sanctions, coding accuracy for services rendered, and admission necessity reviews. Additionally, Livanta monitors Physician Acknowledgement Statements (PAS). Livanta employs a medical review application within CompassWeb to facilitate and manage these reviews. The information collected and maintained in CompassWeb is retained for the duration necessary to complete a review and resolution, following CMS QIO retention guidelines. BFCC-QIO Medicare case reviews are initiated through a phone call, fax, or letter from a beneficiary, a beneficiary representative, a state agency, or other referral sources. At this stage, all relevant beneficiary demographic information is entered into CompassWeb's predefined fields, including name, date of birth, mailing address, phone number, Medicare Beneficiary Identifier (MBI), Health Insurance Claim Number (HICN), phone number, and review notes. Signed complaint and representation forms are subsequently obtained from the beneficiary or beneficiary representative, where applicable, and are added to the imaging section of CompassWeb. Beneficiary medical records requests and responses are exchanged with the provider, and these records, including medical record numbers, legal documents (e.g., powers of attorney), and device identifiers, are added to CompassWeb. Provider information, such as name, contact information, address, National Provider Identifier, Medicare provider number, phone number, and fax number, is also entered into CompassWeb. Livanta logs information regarding provider interactions into the system. For claim review services, authorized Livanta employees and approved

subcontractors utilize CompassWeb to review various medical documents and Medicare claims to determine the accuracy of coding and claim status (inpatient vs. outpatient) for services. Authorized Livanta employees and approved subcontractors use CompassWeb to record and share notes, questions, and decisions for both case and claim reviews. For case and claim reviews, they also use CompassWeb to compose, send, and store determination letters to providers and beneficiaries. Additionally, for both case and claim reviews, Livanta authorized employees and approved subcontractors use CompassWeb to generate reports on statistical and other management data. This information is typically available indefinitely, but in all cases, it will be available for at least six years from the decision date. Access to the CompassWeb system is restricted to authorized Livanta employees and approved subcontractors through multifactor authentication, which includes a username and password. Once entered, a time-sensitive code is emailed to the user's predetermined email address. The user must then enter the code to gain access to the system.

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

Yes

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

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Legal Documents

Device Identifiers

Employment Status

Health Insurance Claim Number (HICN); Medicare Beneficiary Identifier (MBI); access credentials (username and password); review notes; correspondence with beneficiaries; correspondence with medical providers; correspondence with Medicare contractors; correspondence with CMS; National Provider Identifier; Medicare provider number; and fax number. Date of Death, Therapy Records

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

Public Citizens

Vendor/Suppliers/Contractors

Patients

Medical providers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose of Personally Identifiable Information (PII) within CompassWeb is to identify Medicare beneficiaries and create case files to determine whether healthcare providers provide proper healthcare and medical treatment and if claims are coded correctly. PII is also utilized to generate reports on statistical and other management data. Additionally, PII is used by authorized employees and approved subcontractors to access the CompassWeb system and facilitate CMS contract obligations.

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.

Sections 1152-1154, 1156, 1160, and 1171-1179 of the Social Security Act; Section 264(c) of the Health Insurance Portability and Accountability Act of 1996; and Regulations at 42 CFR Part 480 and 45 CFR Parts 160, 162, and 164.

5 USC Section 301, Departmental Regulations

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.

09-70-0536 - Medicare Beneficiary Database, published 12/6/2001 and updated 3/7/2006 and

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Identify the OMB information collection approval number and expiration date

Other CMS Form 10287, Medicare Quality of Care Complaint Form: OMB Control #: 0938-1102, as amended
Governmental Sources CMS-1696, Appointment of Representative: OMB Control #: 0938-0950, as amended
Other Federal EPT 03/2025

Non-Governmental Sources

Public

Private Sector

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Memorandums of Agreement (MOAs) are in place with all Medicare healthcare providers, payer organizations, and state agencies responsible for licensing healthcare providers. Subcontracts are in place with all approved Livanta physician reviewers. There are Joint Operating Agreements with Medicare contractors. CMS has Computer Matching Agreements (CMA) with other federal agencies for the sharing or disclosure between the agencies.

Describe the procedures for accounting for disclosures.

Disclosures are by phone, fax, and letter. Each disclosure is logged within four days of occurrence in the CMS designated system.

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

During the intake process, callers are informed verbally that their personal information is being collected and required to establish a case file. Livanta users are advised as part of the employment process, that the company will collect and retain their personal information.

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.

There is no 'opt-out' option for the collection of PII as it is inherent to the QIO review process to create a review case and perform review of the case. Compass Web users cannot opt-out of providing access credentials, as they are required to use Compass Web.

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

No process exists for notifying individuals about major changes to system disclosure or data uses because no such major changes are anticipated.

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.

Should any individual express such a concern, the individual would be referred to the Livanta ethics website to report a potential violation, and/or the incident would be reported to senior management for resolution.

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

During each contact with individuals whose PII is in Compass Web, Livanta reconfirms the information on file to ensure the integrity, availability, accuracy, and relevancy. In addition, the following security measures are in place to support the data's confidentiality, availability and integrity: encryption in transit and at rest; routine system account reviews, daily back-up of data; limitation of access by authorized users; system activity logs centrally stored with daily monitoring by security personnel; and annual security and privacy training.

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.

Compass Web uses Role Based Access controls which include multifactor authentication using both passwords and revolving codes which change every 30 seconds. These controls are centralized and monitored by a team of system security specialists. Audit records are retained for all account access, changes, and deletions.

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.

Livanta employs stringent pre-screening measures on all system users. The system uses role-based access controls at the network level and application level. Compass Web is a closed system, meaning it cannot be directly accessed from the Internet. Several control layers are put in place, such as: all users must have an active domain account; be assigned a dedicated Workspace (virtual

PC); register for a Livanta credential ID to allow for multifactor authentication; and have a valid Compass Web account.

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 Livanta members must undergo a series of privacy and security awareness training modules before they can access any Livanta systems. Awareness alerts are communicated to all staff regularly or as new or developing threats arise. Refresher trainings are conducted at least annually for all active staff members.

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

Not applicable

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.

Compass Web follows the CMS Record Schedule, more specifically the Center for Clinical Standards and Quality (CCSQ) File Plan. This is inherited from the National Archives and Records Administration (NARA). The National Archives and Records Administration (NARA) has helped develop recommendations for improving the administration of the Federal Advisory Committee Act (FACA), Freedom of Information Act (FOIA), Information Technology (IT), transitory files, travel, records management, forms management, and Contract Officer Representative (COR) information and responsibilities. The disposal authority for Compass Web is N1-440-09-3 and calls for destruction of data after 10 years or when it is no longer needed for agency business, whichever is later.

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

Compass Web is operated inside the federally accredited Amazon Web Services (AWS) data center. Within AWS, Livanta maintains its own virtual private cloud. Only authorized Livanta staff members can access these systems. There are stringent pre-screening measures, ongoing security training, and role-based access controls.

Technically, Compass Web is a closed system, meaning it cannot be directly accessed from the Internet. Livanta has placed the following control layers in place: users must have an active account, users must have dedicated workspaces (virtual PCs), and users must have valid credential IDs registered to Livanta for multifactor authentication measures. Additionally, staff members must have valid Compass Web accounts to access the main application. Data is encrypted in transition and at rest. Data is also backed up daily.

The AWS facility has controlled access by using security guards and identification cards to prevent unauthorized access. The facility is also video monitored.