US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/04/2017

OPDIV:

CMS

Name:

COMPASS WEB

PIA Unique Identifier:

P-8056478-878050

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

Livanta LLC (Livanta) is a Beneficiary and Family Centered Care Quality Improvement Organization (BFCC - QIO) that contracts with CMS to perform reviews of Medicare beneficiary appeals and complaints about healthcare treatments, reviews of the quality of care and Medicare providers. Livanta is one of two BFCC-QIOs in the US and manages Areas 1 and 5, which consists of 19 states and US territories.

CompassWeb is the internal database application/system used by Livanta to support those services.

CMS relies on QIOs to improve the quality of healthcare for all Medicare beneficiaries. QIOs are authorized under Title XI Part B and Title XVIII and Sections 1152-1154 of the Social Security Act. The QIO Program is an important resource in CMS’s effort to improve 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 beneficiary information: names; dates of birth; mailing addresses; phone numbers; medical records; medical records numbers; legal documents (e. g., powers of attorney); device identifiers; employment status; and Health Insurance Claim Numbers (HICN).

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.

CompassWeb is used to record and share notes from Livanta LLC staff, as well as remote physician reviewers. Additionally, CompassWeb is used to compose, send, and store decision letters to providers and beneficiaries, and run reports on statistical and other management data.

The Compass Web system is a Livanta maintained, stand alone system. Livanta LLC staff are not direct contractors of CMS and do not have HHS credentials. However, the system stores the required user identities and credentials for its authorized Livanta users. No CMS employees access the system.

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

As a BFCC-QIO, Livanta performs numerous types of Medicare beneficiary healthcare reviews that include, but are not limited to the following: quality of care reviews, including beneficiary complaint reviews and general quality of care reviews; beneficiary appeals of denials of hospital admissions, discharge and terminations of services decisions, commonly referred to as Grijalva, Benefits Improvement & Protection Act (BIPA) and Weichardt appeals; medical necessity reviews; reviews of EMTALA services; sanctions; and monitoring of Physician Acknowledgement Statements (PAS).

To facilitate and maintain those reviews, Livanta utilizes a medical review application known as CompassWeb. The information collected and maintained in CompassWeb is retained for the length of time necessary to complete a review and resolution, subject to QIO Manual guidelines.

BFCC-QIO Medicare review cases start with a phone call or letter from a beneficiary, at which time all pertinent beneficiary demographic information is entered into CompassWeb’s predefined fields, including name, date of birth, mailing address, phone number, Health Insurance Claim Number (HICN), phone number, and review notes. Signed complaint and representation forms are later obtained from the beneficiary and are added to the imaging portion of CompassWeb. Beneficiary medical records requests and replies are exchanged with the provider, and those records, including medical records numbers, legal documents (e.g., powers of attorney), device identifiers, and employment status, are added to CompassWeb as well. Provider information, such as name of provider, names of contacts, address, National Provider Identifier, Medicare provider number, phone number, and fax number are entered into CompassWeb as well as Livanta's contacts with the providers.

CompassWeb is then used to record and share notes, questions, and decisions from Livanta LLC staff, as well as remote physician reviewers. Finally, CompassWeb is used to compose, send, and store decision letters to providers and beneficiaries, and run reports on statistical and other management data. This information will be available indefinitely, but in all cases at least six years from the date of the decision.

Livanta employees and approved physician reviewer subcontractors access the system through multifactor authorization that includes a username and password. Once entered, a time-sensitive code is emailed to the user's predetermined email. The user is then required to enter the code to achieve access to the system. Only approved Livanta employees or approved physician reviewer subcontractors access the CompassWeb system.

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

Legal Documents

Device Identifiers

Employment Status

Other: Health Insurance Claim Number (HICN); Access credentials (user name and password);

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

Public Citizens

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of PII within CompassWeb is to identify Medicare beneficiaries and create case files to determine if proper healthcare and medical treatment is being given to the individuals by healthcare providers. PII is also used to run reports on statistical and other management data. Additionally, PII is used by CompassWeb for authorized users to access the system.

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.

5 USC Section 301, Departmental Regulations

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

Online

Government Sources

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

CMS Form 10287, Medicare Quality of Care Complaint Form

OMB Control #: 0938-1102, expiration 03/31/2017

Form CMS-1696, Appointment of Representative

OMB Control #: 0938-0950, expiration 6/30/2018

Is the PII shared with other organizations?

Yes

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

Within HHS

Information may be shared with the HHS Office of the General Counsel to support HHS litigation positions. Information may also be shared with the HHS Office of the Inspector General to allow that agency to consider sanctions, such as expulsion from the Medicare program, for gross and flagrant violations or continued substantial violations of medical standards of care when treating Medicare patients.

Other Federal Agencies

Information may be shared with the Department of Justice, for the enforcement of Medicare laws.

State or Local Agencies

Information may be shared with State departments of health, and the state survey agencies that survey medical facilities for compliance with certification requirements.

Private Sector

Information may be shared with Medicare beneficiaries themselves and their duly- authorized representatives, as well as physicians in clinical practice with whom Livanta subcontracts to perform independent reviews of medical records in accordance with duties under the contract Livanta has with CMS.

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

Memorandums of Understanding (MOU) are in place with all Medicare healthcare providers, payer organizations and State agencies responsible for licensing healthcare providers. MOUs are also in place with all approved physician reviewers.

There are Joint Operating Agreements with Medicare Administrative Contractors and State agencies. 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 as part of the reporting of decisions and responses to complaints about the quality of care Medicare beneficiaries receive. Each disclosure is logged within four days of occurrence in both the CMS Case Review Information System and the BFCC-QIO's CompassWeb system for case tracking and management.

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. CompassWeb users cannot opt-out of providing access credentials, as they are required to use CompassWeb.

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 which 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.

Users:

Account reviewers, managers, and approved physicians have access to PII to create, process and manage the Medicare beneficiary cases.

Administrators:

The IT administrators may access PII, in order to maintain and ensure proper functionality of the systems.

Developers:

Senior Software Developers may access PII, in order to maintain the applications and ensure the integrity of the data.

Contractors:

Livanta sub-contractors may access PII, in order to maintain and ensure proper functionality of the Compass Web systems. Contracted Physician Reviewers access PII in order to conduct case reviews in accordance with the QIO statement of work.

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

CompassWeb 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. CompassWeb 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 CompassWeb 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 Achieves and Records Administration (NARA). NARA has recently made change to 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 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.

CompassWeb is operated inside the federally accredited Amazon Web Services (AWS) data center. Within AWS, Livanta maintains their 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, CompassWeb is a closed system, meaning it cannot be directly accessed from the Internet. Several control layers are put in place: users must have an active account, a dedicated Workspace (virtual PC), and a valid credential ID registered to Livanta for multifactor authentication measures. Additionally, staff members must have a valid CompassWeb account to access the main application. Data is encrypted in transition and at rest and backed up daily.

The facility has controlled access by security guards and identification cards. The facility is also video-monitored.