FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

Division of Administration (DOA) use of

EyeMed Vision Care LLC

EyeMed

Date Approved by Chief Privacy Officer (CPO)/Designee: 1/28/2019

PTA/PIA TEMPLATE VERSION 1.9 – August 2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Federal Deposit Insurance Corporation (FDIC), Division of Administration (DOA), Human Resources Branch manages the Agency's benefits plans. These plans provide health, dental, life insurance, disability, and vision benefits to FDIC employees and their eligible dependents through the collection and processing of plan participant information obtained through electronic or paper-based means. The FDIC is publishing this Privacy Impact Assessment (PIA) to broadly cover the collection, use, maintenance, retrieval, and dissemination of personally identifiable information (PII) of FDIC employees and eligible dependents for the purpose of administering the FDIC Vision Plan via EyeMed Vision Care LLC (EyeMed).

The FDIC DOA's Human Resources Branch is responsible for administration of the FDIC Vision Plan. This plan is a component of the FDIC Choice, an Internal Revenue Code (IRC) Section 125 Flexible Benefits Cafeteria Plan. Upon hire, or as a result of a qualifying life event[1], FDIC employees have the option to enroll in the FDIC Vision Plan or the Office of Personnel Management's (OPM) Federal Employees' Dental and Vision Insurance Plan (FEDVIP) for vision benefits. A significant number of FDIC employees choose the FDIC Vision Plan due to cost-savings.

FDIC employees enroll in the FDIC Vision Plan by logging into their MyEnroll.com[2] accounts. Once signed-in, FDIC employees receive a system notification informing them that they are accessing a government system and use of the system requires consent to monitoring and recording. FDIC employees must affirm or deny their consent. FDIC employees who do not consent to the use of the MyEnroll.com system have the option to have benefits specialist enroll them.

After consent is affirmed, the MyEnroll.com system takes FDIC employees to their Employee Home Page. The Employee Home Page allows FDIC employees to review their personal information for errors. The personal information included in the Employee Home Page includes: name, unique identifier, home address, Social Security number (last four digits shown but can be revealed when editing), date of birth, work and personal email addresses, and work and personal telephone numbers. The Employee Home Pages also contains information on FDIC employees' dependents. The information on FDIC employees' dependents includes name, date of birth, and Social Security number. After the review of personal and dependent information is completed, FDIC employees click on the "Open Enrollment" banner to make vision and other benefit selections.

The FDIC Vision has two options for vision insurance coverage: the Vision Standard or Vision High option. The main difference between the Vision Standard and the Vision High option is cost of the plan premiums and co-payments for vision services. After FDIC employees make their vision and other benefits selections, they are taken to a summary page. The details of benefit selections and their associated costs are displayed on the summary page. FDIC employees must review their selections and click "Submit" in order for their selections to be confirmed. The MyEnroll.com system exports vision plan information to EyeMed on a two-week rolling basis.

The FDIC DOA's Human Resource Branch has contracted with EyeMed to administer the FDIC Vision Plan for eligible employees and their dependents. EyeMed is a covered entity under the Health Insurance Portability and Accountability Act (HIPAA) and subject to its Privacy and Security

[1] For more information, please see the FDIC Life Event guidance located at https://www.opm.gov/healthcare-insurance/healthcare/reference-materials/reference/enrollment/.

[2] FDIC Benefit Specialists input all FDIC employee data contained in MyEnroll.com. MyEnroll.com is a product of Benefit Allocation Systems. The FDIC employee data comes from various FDIC HR forms completed the employee.

Regulations.[3] EyeMed utilizes its Facets Medical application, a proprietary software application for vision insurance administration. The Facets Medical application ingests FDIC employees' vision plan selections as well as personal and dependent information sent securely via the MyEnroll.com system. The Facets Medical application also processes vision claims from vison care providers. Vision claims contain medical information.

When EyeMed receives FDIC employees' vision plan, personal, and dependent information, they mail each FDIC employee their vision insurance cards (with Member ID numbers), a summary of their vision benefits, EyeMed's Notice of Privacy Practices,[4] and a listing of in-network providers near the FDIC employee. Before FDIC employees and their dependents can use their vision benefits, EyeMed requires plan participants to confirm receipt of the vision insurance card. Plan participants must call a toll-free number and provide their zip code and date of birth in order to confirm receipt of their vision insurance card. FDIC Vision Plan participants must present their insurance cards to vision care providers in order to utilize their vision plan benefits. After vision care services are performed, the vision care provider submits a claim to EyeMed for payment. Processed claims are made available in plan participants' online accounts.

EyeMed invites plan participants to voluntarily create an online account via eyemed.com or EyeMed's mobile application[5]. FDIC Employees and dependents (age 18 and older) may create an account for the purpose of viewing benefits and service information. FDIC Employees can only view the accounts of dependents who are minor children. To register for an account, plan participants must provide their name, email address, date of birth, and the last four digits of their Social Security number. Additionally, plan participants must confirm their email address to complete registration. EyeMed sends an eight digit pin number to the email address of the plan participant. The plan participant then enters the pin number in the registration portal. When the pin number is authenticated, the plan participant's account is created.

Because the FDIC has not assessed the security controls of the mobile application, there is a privacy risk that the EyeMed mobile application does not have sufficient administrative, physical, and technical controls to protect the confidentiality, integrity, and availability of FDIC Vision Plan participants' PII. This risk is mitigated by the fact that EyeMed manages, transmits, retains, and maintains all plan participants PII in accordance with HIPAA regulations and the National Institute of Standards and Technology (NIST) Special Publication 800-53.[6] EyeMed is contractually obligated and has various mechanisms in place to ensure that PII is used in accordance with these guidelines. Lastly, EyeMed is required to maintain IT solutions using compliant security controls that fully address FDIC and Federal IT security and privacy requirements for systems that transmit and maintain PII.

SECTION II – DATA TYPE, SOURCES, AND USE

[3] Covered entities must comply with the HIPAA Privacy Regulations found in 45 CFR Part 160 and Subparts A and E of Part 164 as well as the HIPAA Security Regulations found at 45 CFR 160 and Subparts A and C of Part 164.

[4] A Notice of Privacy Practices tells individuals how health providers and health plans may use and share their health information. It must also include a statement regarding health privacy rights. In most cases, individuals should receive the notice on their first visit to a provider or in the mail from their health plan. Individuals may also ask for a copy at any time. For more information, please see https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html.

[5] The mobile application can be downloaded on your smartphone by utilizing the Apple App Store or the Google Play Store.

[6] NIST 800-53 outlines the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. For more information, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

FDIC
The FDIC DOA maintains the following information in the MyEnroll.com:

- ***FDIC Employee***
  - Name;
  - Home and work addresses;
  - Home and work telephone numbers;
  - Social Security Number;
  - Date of Birth; and
  - Unique identifier.

- ***FDIC Employee Dependents***
  - Name;
  - Address (if different from FDIC Employee);
  - Social Security Number; and
  - Date of Birth.

EyeMed
The EyeMed Vision Care LLC maintains the following information in their proprietary software:

- Plan participant's name;
- Plan participant's Social Security Number;
- Plan participant's Date of Birth;
- Personal email address;
- Member ID;
- Medical information; and
- Plan participant benefit information.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

EyeMed collects, uses, and maintains the PII of FDIC Vision Plan participants for two purposes: (1) to administer the Agency's vision insurance plan; and (2) for account creation for plan participants. PII of FDIC employees and their dependents are securely imported from the MyEnroll.com system. Employees and their dependents (age 18 and older) may create an account in the application for the purpose of viewing benefits and medical information. Employees can only view the accounts of dependents who are minor children. Vision care service providers' processed claims are uploaded to the plan participants' online accounts. Lastly, the privacy risks associated with EyeMed's mobile application is mitigated by contractual obligations that mandate EyeMed's adherence to federal privacy and security requirements.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above?

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☐	☒
Social Security Number	☒	☐
Employment Status, History or Information	☐	☒
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☒	☐
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☐	☒
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐	☒
Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: _____)	☐	☒

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs:
SSNs are required to accurately identify the employee for purposes of benefit eligibility.

b) Provide the legal authority which permits the collection of SSNs.
Executive Order 9397, as amended.

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service:
SSN is truncated in the EyeMed web-portal and application; and available in its entirety while FDIC employees are updating their personal information in MyEnroll.com.

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☒	7,501 – 10,000 ☐	10,001 – 50,000 ☐	50,001 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[7]:

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[8] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
MyEnroll.com	Social Security number, Unique Identifier, Date of Birth, name, home address, eligible family members – name, SSN, and DOB	☒ Yes ☐ No
Entered manually by eligible employee/dependent	First name, last name, DOB, member ID or last 4 digits of SSN. An employee can create a member account in EyeMed to view/monitor their account information. The employee can also view account information for covered family members under the age of 18.	☒ Yes ☐ No
Collected from eye care provider	Description of services provided and prescription information is entered using designated service codes.	☒ Yes ☐ No

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

The FDIC and EyeMed retrieve employee and dependent vision benefit information by personal identifiers listed in Question 7.

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

The system operates and is covered under FDIC-30-64-0014 Personnel Benefits and Enrollment Records SORN.

[7] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[8] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will access or receive PII data as part of the outsourced service/project.

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	EyeMed is contracted to administer a vision plan for FDIC. FDIC business data is not collected, retrieved through data transfer or stored in any EyeMed application. PII is retrieved through data transfer from MyEnroll.com system.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	FDIC employees may create an account to access their eye care information and the information related to eligible minor family members.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☒	☐	Dependents may voluntarily create an online account via EyeMed.com or EyeMed's mobile application. The information collected from dependents are listed in Section II.
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☐	☒	
10e. Federal, State, and/or Local Agencies	☐	☒	
10f. Other	☒	☐	

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☐	☒
FDIC Confidentiality Agreement (Individual)	☒	☐
Non-Disclosure Agreement (NDA)	☐	☒
Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: _____)	☐	☐
If you answered NO to any item above, please provide additional information if available: The FDIC Legal Division determined that the FDIC Confidentiality Agreement was the only agreement required.		

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information.

☒ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information.

The FDIC Vision Program is a benefit offered to employees. Employees have the option to opt out of the program.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☒ Yes
- ☐ Link to FDIC Privacy Policy
- ☐ FDIC Privacy Act Statement
- ☒ Contractor Privacy Policy or Statement
- ☐ No Privacy Policy has been posted

☐ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care.

☒ EyeMed Vision Care LLC has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☒ YES

☒ The FDIC conducts background investigations (BIs) on key EyeMed Vision Care LLC personnel and other applicable personnel prior to their beginning work on the contract.

☒ The EyeMed Vision Care LLC is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsource Service Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

☒ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form*.**

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date?

☐ Data is collected directly from individuals and/or from the failed financial institutions. As such, the FDIC and its vendors rely on the individuals and/or financial institutions to provide accurate data.

☐ The vendor/contractor works with FDIC to verify the integrity of the data [before, in conjunction with, and/or after] inputting it into the system or using it to support the project.

☐ As necessary, an [authorized user or administrator] of the [System/Project Name] checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☒ Other (*Please explain*.) Data is transmitted from the MyEnroll.com system. The MyEnroll.com system performs dependent eligibility audits to keep information current.

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider.

☒ Within FDIC, the EyeMed Vision Care LLC Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated National Account Manager to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

EyeMed's application, Facets Medical, is on an encrypted platform. EyeMed encrypts its databases as well as its backup tapes. Additionally, routers enforce access controls and implements firewalls around the data. Firewalls have real-time logging and alerting capabilities.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

Upon completion or termination of the contract, or at any time the Contracting Officer requests in writing, Contractor shall return all FDIC information on any media under its control or in its possession, as FDIC directs. All FDIC information shall be destroyed in accordance with Federal and State regulatory requirements.