FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

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

for

Employee Benefits Management Services

(EBMS)

FDIC PRIVACY PROGRAM

Date Approved by Chief Privacy Officer (CPO)/Designee: November 26, 2013

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

When a financial institution fails, and the Federal Deposit Insurance Corporation (FDIC) is appointed as its Receiver, the FDIC/Receiver is obligated[1] to provide continuation of health insurance coverage to the employees[2] of the failed institution ("Qualifying Beneficiaries"/"Participants"). The continuation coverage, known as "FIA" (FDIC Improvement Act of 1991, Section 451), is the FDIC-sponsored generic health plan that is intended to comply with Section 451 and the requirements of Section 602 of the Employee Retirement Income Security Act (ERISA) of 1974. The FDIC is contracting the services of Employee Benefits Management Services ("EBMS"), a Third Party Administrator (TPA), to administer this group health plan.

The TPA is responsible for providing the following services under the contract:

1. Sending notification letters, benefits enrollment/election material, and other applicable correspondence[3] to qualifying beneficiaries/participants.
2. Collecting enrollment/election forms and premiums from qualifying beneficiaries/participants and informing them about new premiums.
3. Remitting premiums to FDIC's account established for such purpose (no PII involved).
4. Generating Reports for FDIC, including:
    a. Monthly Reports detailing the billing status of all participants in the FIA Health Insurance Continuation Coverage Plan. A separate claims and premium record for each failed financial institution with active FIA Plan participants will also be provided by the TPA to the FDIC. Such reports may include minimal PII, such as participant name, provider name, and amount of claim.
    b. Special Management Information Reports containing customized management information provided upon FDIC's request. These reports will not contain any PII.
5. Performing Claim Services, such as:
    a. Receiving claims and processing payment of benefits for participants in accordance with the FIA Health Insurance Continuation Coverage Plan.
    b. Corresponding with the participants and Providers of Services, if additional information is deemed necessary to complete the processing of claims, via first-class mail.
    c. Determining the amount of benefits payable under FIA Health Insurance Continuation Coverage Plan.
    d. Coordinating benefits payable under the FIA Health Insurance Continuation Coverage Plan with other benefits plans, as applicable.
    e. Providing notice to participants as the reason(s) for denial of benefits and providing for the review of claims that are denied, via first-class mail.

[1] Section 451 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FIA) mandates the continuation of health plan coverage in cases of failed financial institutions.

[2] This includes (1) Active employees (and their eligible dependents) who were enrolled in the plan date of closure of financial institutions; (2) Retired employees and their eligible dependents who lost coverage due the failed financial institutions closure, except those who are covered by Medicare or Medicaid; and (3) Employees (and their dependents) who worked for the failed institution and are currently covered by COBRA or are within their 60 election period to elect COBRA.

[3] Notification provided by the TPA may include: (a) Initial Notices: Notices are sent via first class mail to Qualifying Beneficiaries describing FIA Continuation Coverage benefits available and how they may obtain coverage; (b) New Employees: On behalf of FDIC, the TPA will send notices by first class mail to new employees upon activation of FIA Health Insurance Continuation Coverage; (c) Coverage Election: Upon written notification by FDIC of a Qualifying Event under FIA Health Insurance Continuation Coverage, the TPA will send a notice via first class mail to the employee's current address, as furnished by the FDIC. This notice will describe the FIA Health Insurance Continuation Coverage benefit options and premiums designated by the FDIC. The TPA will solicit election or non-election decisions on a form by first class mail to be retained as evidence of the Qualifying Beneficiary's election decision; (d) Additional Notices: Upon written notification by FDIC, the TPA will send a notice via first class mail to Qualifying Beneficiaries and to Participants to announce benefits changes, coverage options and other events pertinent to FIA Health Insurance Continuation Coverage, including but not limited to notification requirements as required by the America Recovery and Reinvestment Act (ARRA).

As part of the above services provided under the contract, the TPA (EBMS) will collect and maintain sensitive personally identifiable information (PII) about qualifying beneficiaries/participants, including full names, dates of births, Social Security Numbers (SSNs), home addresses, medical information, and other PII specified in Q4. The TPA will store the qualifying beneficiary files in its secure systems and hardcopy files for the duration of the contract and as required by FDIC document retention guidelines. For more information about how the TPA will collect, use and protect this sensitive PII, please refer to Sections II thru VI of this Privacy Impact Assessment (PIA).

2. Status of the Outsourced Information Service Provider:

- ☐ Solicitation/On-Boarding (Pre-Award; or At/Around the Time of Contract Award)
- ☒ Initial Assessment/Due Diligence (Post-Award)
- ☐ Ongoing Monitoring of Contract (Post-Award)
- ☐ Sunset or Disposition of Contract (Post-Award; At or Near Contract Expiration)
- ☐ Other (*Explain*):

SECTION II – INFORMATION TYPE, SOURCES, AND USE

3. Will the Outsourced Information Service Provider collect, maintain or generate Personally Identifiable Information (PII) about individuals on behalf of FDIC? ☐ NO ☒ YES *(If yes, check ALL categories that apply. This is not intended to be an all-inclusive list. Specify other categories of individuals, as needed.)*:

☐ FDIC Employees	☐ Borrowers/Customers of Failed Financial Institutions
☐ FDIC Contractors	☐ Claimants (Depositors or Non-Depositors)
☐ FDIC Visitors	☐ Receivership Payees or Payers*
☐ Complainants	☒ Failed Bank Officers/Directors/Employees
☐ Requestors	☐ Failed Bank Creditors or Vendors*
☐ Bidders or Investors*	☐ FDIC Business Customers/Vendors*

☒ Other *(Specify):* Eligible Dependents of Failed Financial Institution Employees

☐ NONE *(No PII about individuals will be collected, maintained, or generated.)*

***Note: The asterisk is equivalent to individuals NOT businesses.**

4. What specific types of PII will the Outsourced Information Service Provider collect, maintain or generate on behalf of FDIC? Also, what are the Sources of the PII? *(Check applicable box(es) below. This is not intended to be an all-inclusive list. Specify other categories of PII, as needed.)*:

PII Element	Entered manually by authorized users	System-generated	Collected directly from individuals thru a form or other mechanism	Collected from FDIC staff, system(s)/ application(s)	Collected from non-FDIC entities, system(s), or application(s)	Collected from federal, state, or local gov't agencies	Other collection method or mechanism
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 ID Number	☐	☐	☐	☐	☐	☐	☐
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)	☐	☐	☐	☐	☐	☐	☐
NONE.	☒	☒	☐	☐	☒	☒	☒
Other (Specify): Gender	☐	☐	☒	☒	☐	☐	☐

5. How will the PII Elements in question 4 be *derived* from each Source? (*Provide specific details about who will provide the PII and how in the applicable columns below*).

5a. Entered manually by authorized users	Not applicable.
5b. System-generated	Not applicable.
5c. Collected directly from individuals thru a form or other mechanism	**Qualified Beneficiaries/Participants –** In order to administer the FIA group health plan, authorized TPA staff may collect sensitive PII data directly from qualifying beneficiaries/participants (i.e., eligible employees of failed financial institutions and their dependents). This data may be received from beneficiaries/participants via multiple communication methods including the TPA's secure email service, phone, fax, first-class mail, and via the TPA's secure web portal (www.ebms.com). The PII is derived from benefits enrollment/election forms, benefits claims, premium payments, and other correspondence and information provided by beneficiaries/participants to the TPA. The data provided by participants may include their full names, dates of births (DOBs), Social Security Numbers (SSNs), home addresses, medical information, and other PII data specified in response to Question 4.
5d. Collected from FDIC staff, system(s)/ application(s)	**FDIC/DRR Claims Staff** – During a bank closing, authorized FDIC/DRR Claims staff collect benefits data from the failed financial institution's human resources department and prepare a FIA list/spreadsheet, which contains the following PII about qualifying FIA beneficiaries/ participants (i.e., eligible employees of the failed financial institution, their dependents, and COBRA employees and Retiree participants): full names, SSNs, DOBs, gender, and home addresses, and medical information (i.e., whether they are eligible for health, dental or vision care under the FIA plan; effective date of COBRA (for COBRA employees); and insurance coverage paid to date (for retirees). Authorized FDIC/DRR Claims staff either save the FIA list on a secure FDIC network drive or securely email it to their own account via an encrypted VPN connection from the failed financial institution to the FDIC network. FDIC/DRR Claims staff then securely email the FIA list for qualifying beneficiaries to the FDIC FIA Contact for their office who reviews and sends the data to the TPA via FDIC's secure email service. The TPA retains the FIA list/spreadsheet in its secure system and/or hardcopy paper files.
5e. Collected from non-FDIC entities, system(s), or application(s).	Not applicable.
5f. Collected from federal, state, or local government agencies	Not applicable.
5g. Other collection method or mechanism	Not applicable.

6. What will be the intended use and purpose of the PII identified in question 4? *(Provide a summary of how the PII will be used by the Provider in support of a specific FDIC business process.)*

The PII identified in Question 4 (above) is collected in accordance with the Federal Deposit Insurance Corporation Improvement Act of 1991 (FIA) that mandates the continuation of health plan coverage for employees of failed financial institutions. To ensure the group health plan meets the requirements of section 602 of the Employee Retirement Income

Security (ERISA) Act of 1974, the TPA will act as the administrator of the group health plan and administer the health plans on behalf of the FDIC.

7. Will system users *retrieve* data or records in the system by a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

☐ Not Applicable ☐ No ☒ Yes *(If yes, explain how data is retrieved.)*

8. Explanation: Records may be retrieved in the TPA's system by name and last four digits of the Plan Participant's social security number.

SECTION III – ACCESS AND SHARING

9. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will have access to, or be provided with, PII data as part of the outsourced service. *(Check "No" or "Yes" for each category. For each category checked "Yes," specify who will have access to the PII, what PII elements will be accessed/shared by them, how the access or sharing will occur, and the purpose and use of this PII.)*

PII Will Be Used By and/or Shared With:	No	Yes	If Yes, Explain the Purpose and Use of PII
9a. FDIC Employees	☐	☒	Authorized FDIC/DRR Claims staff members have access to the data collected from the failed financial institution during the bank closing, which includes the sensitive PII about Qualifying Beneficiaries/Participants specified in Q4. The purpose of this collection is to allow continuation of health plan coverage for employees of the failed financial institution in accordance with the FDIC Improvement Act of 1991 (FIA). Once this data is collected, a FIA participant listing is created and sent by authorized FDIC/DRR Claims staff to the FDIC FIA Contact for their office who reviews and sends the data to the TPA via FDIC's secure email service. This data may contain some or all of the PII specified in response to Q4. Authorized FDIC/DRR Claims staff members receive various reports and invoices from the TPA via the TPA's secure website. Certain reports may contain minimal PII, such as the names of plan participants, provider names and claim amounts. FDIC/DRR Claims staff members securely download and retain the reports in their secure electronic and/or hardcopy files.
9b. FDIC Contractors	☒	☐	Not applicable. The TPA is not providing PII to FDIC contractors.
9c. Outsourced Information Service Provider Staff and/or the Information Service Provider's Subcontractors	☐	☒	Authorized staff at the TPA (Employee Benefits Management Services) who administer the group health plan and handle claims have access to the PII specified in Q4 pertaining to employees of the failed financial institution and their eligible dependents. TPA staff receive this PII data from FDIC/DRR Claims staff via secure email and directly from plan participants via the methods noted in response to Q5(c). The TPA is required to handle, maintain and

			protect this data in accord with the information security and privacy standards outlined in their contracts and Confidentiality Agreements with FDIC. In addition, while the TPA is not directly subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements, the TPA does receive and process personal health information from qualifying beneficiaries that is covered by HIPAA. Therefore, the TPA has developed a privacy and security compliance program for its staff that takes into account HIPAA privacy and security standards and reasonable practices in the healthcare industry. In addition, the TPA trains its staff who have access to personal and protected health information in the proper handling and protection of this information.
9d. Other Non-FDIC Entities/Parties (e.g., failed financial institutions, assuming institutions, bidders/investors.)	☐	☒	In order to effectively administer the FIA group health plan, provide customer service and perform claim services, it may be necessary for the TPA (EBMS) to disclose personal and protected health information to authorized third-parties, such as participants' health care providers, hospitals, insurers, service providers and/or business associates. Such information may be made available through enrollment forms, medical claims, medical reports, coverage history and other sources and forms necessary to effectuate claim administration, treatment, payment and health care operations. The information disclosed by the TPA may include participant name, SSN, DOB, home address, personal telephone number, gender, dependent information, and claim information.
9e. Federal, State, and/or Local Agencies	☒	☐	Not applicable. The TPA is not providing PII to government agencies on behalf of FDIC.
9f. FDIC Systems/ Applications	☐	☒	Authorized FDIC/DRR Claims staff save the FIA list, which contains sensitive PII about qualifying beneficiaries/participants as specified in Q4, onto a secure FDIC network drive. In the future, authorized FDIC/DRR Claims staff will upload the FIA list into FDIC's PENTRAX+ application.
9g. Non-FDIC Systems/ Applications	☐	☒	The TPA (Employee Benefits Management Services) maintains the PII data about Qualifying Beneficiaries/Participants in its secure systems called Data Dimension and MTS, and hardcopy files. The TPA stores and transmits personal and protected health information using industry standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction and modification. Certain information containing personal and protected health information that is displayed or received via Internet Web browser technology is transmitted in a secured environment using 128-bit SSL encryption.
9h. Other	☒	☐	Not applicable.

10. If data will be provided to or shared with 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	No	Yes
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 vendor is an outsourced service provider.		

SECTION IV – NOTICE AND CONSENT

If you answered "YES" to question 5C in Section II, answer the following questions:

11. 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. ***(Explain why individuals are not able to opt out (either for specific data elements or specific uses of their data.):*** The PII is collected in accordance with the Federal Deposit Insurance Corporation Improvement Act of 1991 (FIA) that mandates the continuation of health plan coverage for employees of failed financial institutions. This data is necessary for the TPA to enroll and administer qualified beneficiaries under the FIA health continuation coverage plan.

☐ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. ***(Explain how individuals may decline or consent to the use of their information.):***

12. 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 *(If yes, check applicable box(es) below)*

- ☐ 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

13. Please assert what administrative procedures and technical safeguards are in place to protect PII data in the Outsourced Information Service Provider's care. ***[Provide the name of the Outsourced Service Provider and check all applicable box(es).]***

☒ Employee Benefits Management Service will go 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 ☒ PENDING

☒ 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.***

- EBMS has developed a privacy and security compliance program for its personnel that takes into account Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security standards and reasonable practices in the healthcare industry.
- EBMS transmits and stores personal and protected health information using industry standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction and modification. Certain information containing personal and protected health information that is displayed or received via Internet Web browser technology is transmitted in a secured environment using 128-bit SSL encryption.

14. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date? ***[Check all applicable box(es) and insert the appropriate response and System/Project name.]***

☒ Data is collected directly from individuals and 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 in conjunction with 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*.)

15. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider. (*Check all applicable box(es) and insert the name of the Outsourced Information Service Provider and title of the firm's senior management official.*)

☒ Within FDIC, the 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 its Strategic Accounting Officer 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 vendor must comply with the Monitoring and Incident Response 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 – INFORMATION RETENTION AND DISPOSAL

16. Check off all applicable box(es) next to the statements regarding the retention and disposition of data by the Outsourced Information Service Provider.

☐ FDIC records retention requirements have been communicated to the Outsourced Information Service Provider.

☒ The retention period for data used as part of this outsourced service adheres to FDIC requirements for data retention and to those retention requirements noted in the contract.

☐ Data is retired and destroyed in accordance with National Archives and Records Administration (NARA) guidance and FDIC Records Retention and Disposition Schedules. **(NOTE: *Refer to Circular 1210.1, FDIC Records Management Program Manual, for details on how long categories of records may be maintained by the FDIC.)***

☒ If known, please specify the period of time that data is retained and the specific procedures used for disposing of the data.

The data is maintained by EBMS for 7 years in accordance with the Health Insurance Portability and Accountability ACT (HIPAA). After 7 years, the vendor will work with the FDIC Oversight Manager to securely return or destroy this data as advised.