Jacket 742-142

Specifications by WL **Department: DHHS/CMS**
Reviewed by **Requisition: 8-00252**

BID OPENING: January 5, 2009.

Bids shall be publicly opened at 1:00 p.m. prevailing Columbus, OH time on January 5, 2009. Submit bids to: U.S. Government Printing Office, Columbus Regional Printing Procurement Office, 1335 Dublin Road, Suite 112-B, Columbus, OH 43215-7034. **FACSIMILE BIDS ARE ACCEPTABLE.**

Any questions before or after award concerning these specifications call Bill Lansky at (614) 488-4616, Ext. 15. No collect calls.

SPECIFICATIONS

U.S. Government Printing Office (GPO)
1335 Dublin Road, Suite 112-B
Columbus, OH 43215-7034

OFFERS: Offers must include the cost of all materials and operations for the total quantity ordered in accordance with these specifications. In addition, separate prices must be submitted for each additional 1,000 copies of each item. The price for additional quantities must be based on a continuing run, exclusive of all basic or preliminary charges and will not be a factor for determination of award.

FACSIMILE BIDS: Facsimile bids are permitted (see GPO Contract Terms, Pub. 310.2 (Rev. 6-01), Solicitation Provisions, "6. Facsimile Bids"). Submit facsimile bid to FAX: 614-488-4577, or FAX 614-488-9618.

GPO CONTRACT TERMS: Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Pub. 310.2, effective 12/1/87, Rev. 6-01) and GPO Contract Terms, Quality Assurance Through Attributes Program (GPO Pub. 310.1, effective May 1979, Rev. 8/2002).

REGULATIONS GOVERNING PROCUREMENT: The US Government Printing Office (GPO) is an office in the legislative branch of the United States Government. Accordingly, the Federal Acquisition Regulation is inapplicable to this, and all GPO procurements. However, the text of certain provisions of the Federal Acquisition Regulation as contained in the Code of Federal Regulations (CFR), are referenced in this solicitation. The offeror should note that only those provisions of the Federal Acquisition Regulation which are specifically incorporated by reference into this solicitation, are applicable.

PREAWARD SURVEY: In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct a preaward survey or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract.

POSTAWARD CONFERENCE: A conference between contractor and agency is required. The purpose of the conference will be to discuss and review all aspects of the contractor's production plan and to establish coordination of all internal and external operations required to complete this contract. May be done by telephone at governments option.

The Preaward/Postaward Surveys will include a review of all subcontractors involved along with their specific functions, and the contractor's/subcontractor's, personnel, production, security and other requirements outlined in the CMS Data Usage agreement.

PAYMENT: Submit all vouchers to: Comptroller--FMCE, Office of Financial Management, US Government Printing Office, Washington, DC 20401.

SECURITY OF DATA: The contractor shall not release, or sell, to any person any technical or other data received from the Government under the contract; nor shall the contractor use the data for any purpose other than that for which it was provided to the contractor under the terms of the contract.

The contractor must have a detailed Security Plan and submit to the agency personnel upon request. The integrity of any furnished cartridges or electronic submission must be given the highest priority. Therefore, the contractor must guarantee that the furnished addresses will be used only to complete this contract.

NOTE: If handling of furnished address tapes is sub-contracted, security requirements also apply to the sub-contractor as well as the contractor (all parties involved).

SECURITY WARNING: It is the contractor's responsibility to properly safeguard personally identifiable information (PII) from loss, theft, or inadvertent disclosure and to immediately notify the Government of any loss of personally identifiable information. Personally identifiable information includes a person's name, date of birth, Social Security Number, HIC number, address, or benefit payment data.

The contractor will receive a copy of the DUA, Application for Access to CMS Computer Systems) and REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (NON-CMS ONLY)" and Rules of Behavior forms via email, the original copies of each form must be completed and submitted via over night courier within 24 hours of receiving the forms to: HHS/CMS, Attn: Pat McNaughton (410-786-9311), Mail Stop SL-11-16, 7500 Security Blvd., Baltimore, MD 21244-1850. The contractor is encouraged to use FexEx Overnight service.

CONTRACTOR WILL BE REQUIRED TO SIGN AT TIME OF AWARD A "DATA USE AGREEMENT" TO ENSURE THE INTEGRITY, SECURITY AND CONFIDENTIALITY OF INFORMATION MAINTAINED BY CMS. Attachment D, pages 16-21.

CONTRACTOR WILL BE REQUIRED TO SIGN AT TIME OF AWARD A "APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS" FOR FILES TO BE DOWNLOADED FROM CMS COMPUTER SYSTEMS. Attachment E, pages 22-24.

CONTRACTOR WILL BE REQUIRED TO SIGN AT TIME OF AWARD AN "REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (NON-CMS ONLY)". See attached Attachment F, pages 25-28.

CONTRACTOR WILL BE REQUIRED TO SIGN AT TIME OF AWARD A "Rules of Behavior" (See Attachment C, pages 12-15.

SECURITY: See attached Attachment F pages 25-28, "REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (NON-CMS ONLY)". See attached Exhibit G, pages 29-33, "CMS Clause-09A-01 Security Clause – New Contract Awards Date: May 2007" and Exhibit H pages 34-36, "FAQ Supplement to CMS Security Clause 09A-01. Date: April 4, 2008.

The cost of completing the paperwork and forms in E-QIP for the background investigation for two employees must be included in the cost of bid.

PRIVACY ACT NOTIFICATION: This procurement action requires the contractor to do one or more of the following: design, develop, or operate a system of records on individuals to accomplish an agency function in accordance with the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

PRIVACY ACT

(a) The contractor agrees:

(1) to comply with the Privacy Act of l974 and the rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals in order to accomplish an agency function when the contract specifically identifies (i) the system or systems of records and (ii) the work to be performed by the contractor in terms of any one or combination of the following: (A) design, (B) development, or (C) operation;

(2) to include the solicitation notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation when the statement of work in the proposed subcontract requires the design, development, or operation of a system of records on individuals to accomplish an agency function; and

(3) to include this clause, including this paragraph (3), in all subcontracts awarded pursuant to this contract which require the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved where the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency where the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act when the contract is for the operation of a system of records on individuals to accomplish an agency function, the contractor and any employee of the contractor is considered to be an employee of the agency.

(c) The terms used in this clause have the following meanings:

(1) "Operation of a system of records" means performance of any of the activities associated with maintaining the system of records including the collection, use, and dissemination of records.

(2) "Record" means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(3) "System of records" on individuals means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

TECHNICAL SUPPORT: The contractor must have a highly trained technical support staff available around the clock to solve any mechanical and electrical malfunctions. Contractor must also have, on site, a spare parts inventory and on call technicians to avoid any delay in producing orders under this contract plus a Program Manager assigned to the project with designated backup so that a single point of contact will be available to answer any questions which may arise.

TITLE: Personal Health Records Mailer.

Quantity: 755,279 Mailers

The quantities are approximate and the government reserves the right to increase or decrease the quantity by up to +/- 10%. Exact quantity will be furnished with final address files. Billing adjustment due to quantity change will be made at the contractor's "additional" rate.

TRIM SIZE: Item 1 - Mailout envelope 6-1/2 x 9-1/2", plus flap.

Item 2 - Face and back form 8-1/2 x 11" flat, 8-1/2 x 3-2/3" folded.
Item 3 - Face and back form 8-1/4 x 17-15/16" flat, 8-1/4 x 6" folded.

Item 1: Envelope: 6-1/2 x 9-1/2", plus flap. Envelope prints on face with return address in upper left corner and First-Class Mail postage and fees paid permit imprint in upper right corner. Envelope to be open side with diagonal or side seams and a suitable sized gummed flap.

Item 2: Letter: 8-1/2" x 11" Letter prints face and back with type and line in black ink. Trim four sides and fold to 8-1/2 x 3-2/3" with two suitable parallel folds with top of face English side out.

Item 3: Trifold prints face and back, full 100% coverage in 4-Color Process and bleeds all sides.

Variable Imaging (see Attachment A page 11): Item 1 Envelope requires imaging of addresses in black ink using furnished files. Address will be four to six lines. Entire address to be in capital letters with all punctuation deleted.

Contractor to prepare mailing to maximize presort discount and comply with USPS mailing requirement for automations compatible mailing in effect at the time of mailing. The submitted files by CMS have been CASS and NCOA certified. Contractor sponsored address data enhancements to secure postal discount **MUST NOT** negatively affect deliverability and/or omit/change any required address field as provided by CMS address files. It is the contractor's responsibility to keep up to date on all USPS requirements.

See Record Layout and positioning of imaging on Attachment A, page 11.

Contractor is NOT to run Puerto Rico Spanish files through addressing/mailing software. Mail PR/Spanish pieces using USPS First Class non discount/automation rates. Image address information as formatted.

Disposal of Waste Material: The contractor is cautioned that all waste material used in the production of the Notice Letters must be destroyed, i.e. burned, pulping, shredding, macerating, or other suitable means. If the contractor selects shredding as a means of disposal, it is preferred that a cross cut shredder be used. If a strip shredder is used, the strip must not exceed one-quarter inch.

VARIABLE COMPUTERIZED IMAGING:
Contractor will be required to provide variable imaging in accordance with the furnished file record layout sheets. See Attachment A page 11.

Laser image must be a minimum resolution of 600 x 600 dpi.

GOVERNMENT TO FURNISH: PS Form 3615 (Mailing Permit Application and Customer Profile) and GPO Form 712 (Certificate of Conformance).

Item 1: Manuscript copy for the envelopes, contractor to set, match typestyle and weight.

Item 2 & 3: CD-R compact disk, Mac format, in QuarkXpress 6.1, Adobe Illustrator C2, and PhotoShop C2. Files are in native application format. Fonts included. Color laser proof for tri-fold.

It is recommended that the contractor output files on the same platform (i.e. Mac/PC/etc.); no additional time or compensation will be given for errors commonly associated with file output from a different platform. The contractor is responsible for creating or altering any necessary trapping, setting proper screen angles and screen frequency, and defining file output selection for the imaging device being utilized. All furnished files must be imaged as necessary to meet the assigned quality level.

Upon completion of the order, the contractor must return final production native application files (digital deliverables) with the furnished material, along with any final film negatives, if used. The digital deliverables must be an exact representation of the final printed product and shall be returned on a suitable type of storage media.

PREFLIGHT: The contractor shall preflight the furnished disks prior to image processing (i.e. verify completeness and presence of all components required to process image in accordance with the visuals provided such as fonts, bleeds, graphic files, trim size, etc.). Any discrepancies of the Government Furnished Materials (GFM) and these specifications, or instances of missing files, fonts, instructions, etc. are to immediately be brought to the attention of the GPO Contracting Officer prior to further performance.

Identification markings such as register marks, ring folios, rubber stamped jacket numbers, commercial identification marks of any kind, etc., must not appear on finished product.

Data Files will be furnished in the following method:

Electronic file transmission (EFT), the contractor must obtain approval from CMS IT Security for access to CMS computer systems.

Files are furnished by EFT, a Gentran Mailbox will be setup by CMS to provide access to data files. Immediately after award, the contractor must submit two (one primary user, and on back-up user) completed "APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS" at the following internet link: http://www.cms.hhs.gov/InformationSecurity/Dowloads/EUAaccessform.pdf . The contractor must complete Section 2, User Information on page 1, and the Applicant's Information on page 3 on the Form.

Please note that the Applicant's Social Security Number must be provided in order to receive a USERID and gain access to CMS' computer systems. Corporate Tax Identification Numbers are not accepted in lieu of individual SSN's. The contractor must reapply for access every 12 months during the term of the contract.

Return completed form to: HHS/CMS 7500 Security Boulevard, SL-12-17, Attn: Julian Lowery, Baltimore, MD 21244-1850. Phone Number (410) 786-6959. The contractor is encouraged to use FedEx Overnight service. Packages delivered other methods may be opened in the CMS mailroom.

Additional information regarding the CMS EFT Infrastructure can be found at the following link: http://www.cms.hhs.gov/SystemLifecycleFramework/Downloads/EFTInfrastructure.pdf

Software: Contractor will need and Internet browser, the browser must be Internet Explorer 5.0 or above, or you can use GIS-compatible secure File Transfer Protocol Client (FTP).

CONTRACTOR TO FURNISH: All materials and operations, other than those listed under "Government to Furnish", necessary to produce the products in accordance with these specifications.

The contractor must be able to send and receive electronically transmitted data via FTP Protocol. The medium used by the contractor must have the capability to compare records received with records sent, verifying a complete transmission.

PROOFS:

COLOR PROOFS: Submit **2 sets** of one-piece (composite) color proofs, halftone dot quality or color-accurate continuous tone proofs, of complete publication for letter and tri-fold. Color proofs must have illustrations and text matter composited. Low resolution digital proofs (less than 2400 dpi) that are not representative of final image quality and color, as well as film overlay type proofs are not acceptable. Proofs are to be contract quality and be representative of image quality and color that will be matched by the printed press sheets. Any digital proof used as a contract proof must be imaged to predict the appearance of the press sheet, using the same Raster Image Processor

(RIP) that will be used to produce the finished product. The contractor is responsible for providing a control system that facilitates making the match between the approved proofs and the printed press sheets.

LAYOUT/POSITION PROOFS: Also submit **2 sets** of composite layout/position proofs, of the complete publication. Proofs shall consist of a complete product with all elements in proper position (not pasted up), and all pages imposed in correct location, imaged face and back, trimmed, and bound to the finished size of the publication. In lieu of a film based proof (i.e. Dylux, bluelines, etc.), a digital layout proof may be furnished provided that the digital proof is imaged using the same Raster Image Processor (RIP) that will be used to produce the finished product (at a minimum of 600 dpi single color or minimum 400 dpi full color at Contractor's option). Digital layout proofs must also be imaged on two sides and shall accurately predict front-to-back registration and all aspects of page layout/image assembly.

If digital proofs are provided, the make and model number of the proofing system utilized shall be furnished with the proofs.

Delivery of Proofs: Deliver **2** sets of each type of proofs, along with the furnished materials and GPO Proof Memo, directly to CMS, Attn: Pat McNaughton (410-786-9311), Mail Stop SL-11-16, 7500 Security Blvd., Baltimore, MD 21244-1850. All packages containing proofs must be clearly marked on the outside as "PROOFS", and contain the GPO Jacket Number, Requisition Number, and publication title.

All proofs must arrive no later than **January 8, 2009**. All proofs will be withheld not longer than **1** workday(s) from date of receipt, to date proofs are made available for pick up by the contractor (see NOTE below). THE CONTRACTOR MUST NOT PRINT PRIOR TO RECEIPT OF PROOF APPROVAL.

NOTE: It is the responsibility of the contractor to make the necessary pickup arrangements when notified that the reviewed proofs are available. If a courier is to be used, a fully completed airbill (prepaid by the contractor) must be furnished to the specified address with the delivered proofs for this purpose.

VERIFICATION PROOFS:

The contractor is required to e-mail 50 clearly readable randomly selected, password protected .pdf file formatted proofs. Contractor must also submit the corresponding source data files (also known as a "data dump"). The .pdf proofs and data dump must be provided to CMS before an approval will be given to the contractor to begin imaging. If CMS find errors during the proofing process, the contractor must make all corrections and submit additional proofs along with the corresponding source data files. This process will be repeated until the contractor submit samples that CMS considers to be error-free.

Deliver proofs within 2 days of receiving Government files. The Government will approve or disapprove the samples with in 24 hours of the receipt thereof. Notification will be given by e-mail. Approval or disapproval will not relieve the contractor of complying with the specifications and all other terms and conditions of the contract. Additional e-mail samples may be required if the image samples are disapproved.

E-mail envelope proof Pat McNaughton (410-786-9311) PAtrick.McNaughton@cms.hhs.gov and Raymond Wajbel Raymond.wajbel@cms.hhs.gov.

INSPECTION NOTIFICATION: 48 hours prior to start of press, imaging, inserting and mailing operations the contractor must notify GPO Columbus Compliance Unit at 614-488-4616 ext. 0, and CMS Pat McNaughton (410-786-9311).

Press Sheet, Imaging and Inserting inspections will be approved at one location and contractor will be responsible for meeting these standards if more than one production facility is being used. Any data issues with imaging will also have to be communicated between locations by the contractor.

STOCK/PAPER: The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No. 11" dated February 1999. All paper used must be of a uniform shade.

Items 1 (Envelopes): White Writing or Wove Envelopes, grammage 75 - 90 g/m^2 (basis weight: 20 – 24 lbs per 500 sheets, 17 x 22"), equal to JCP Code V20.

Items 2 (letter): White Opacified Offset Book, grammage 90 g/m^2 (basis weight: 60 lbs. per 500 sheets, 25 x 38"), equal to JCP Code A80.

Item 3 (Tri-fold): No. 2 Coated Text:, grammage 150 g/m^2 (basis weight: 100 lbs. per 500 sheets, 25 x 38") equal to JCP Code* A182.

To assure the mailing qualifies for all automation discounts, meets USPS mail quality standards and prevent delays in processing, the color of envelope paper and ink used to address the mailpiece must meet all USPS mail acceptance / automation requirements for *Reflectance and Print* contrast.

Prior to or in conjunction with presenting the mailing for acceptance, a MERLIN (Mail Evaluation Readability Lookup Instrument) mail diagnostics analysis must be completed by the Postal Service. Within 48 hours of acceptance, a copy of the "MERLIN" Summary Verification Reports listing the results must be faxed to CMS, Attn; Ray Wajbel, @ (410) 786-1696.

MARGINS: Item 1: Envelope - Position of all elements per furnished copy, no bleeds. Note: Positioning of all elements on the envelope must be in accordance with all current and applicable USPS DMM requirements.

Item 2: Adequate margins for Letters.

Item 3: Tri-fold bleeds all sides.

TRIMMING/FOLDING/CONSTRUCTION: Item 2: Notice Letter trim 4 sides and fold to 8-1/2 x 3-2/3" (regular "C" or accordion "Z" fold) with two parallel folds, with Letter English side facing out.

Item 3: Tri-fold trim 4 sides and fold to 8-1/4 x 6", regular "C" with two parallel folds.

BINDING/INSERTING:

Insert one copy each of items 2 and 3 into item 1 envelope.

Mailing Envelopes: Envelopes must be prepared and sealed in a manner that will insure acceptance and safe delivery by the U.S. Postal Service.

The contractor must provide all mailing materials, as well as all labeling and marking, as necessary to fulfill mailing and distribution requirements. Noncompliance with the packing and labeling instructions will be cause for the Government to take corrective action in accordance with GPO Pub. 310.2.

VARIABLE COMPUTERIZED IMAGING:

All imaging must be a minimum resolution of 600 x 600 dots per inch and meets quality level III attributes.

Contractor to address using laser or suitable method using a approved font and size in black ink. All address elements, components, ink characteristics and Postnet barcode must meet USPS automated mail processing equipment compatibility standard and comply with all related USPS automated mail processing equipment compatibility standards and comply with all related USPS requirements as sited in the DMM and Standard mail Processing Guidelines in effect at the time of mailing.

ADDRESS REQUIREMENTS: Address placement, format, and fonts must be consistent with current U.S. Postal Service (USPS) *Address Quality Standards,* and in accordance with appropriate USPS rules and regulations including USPS Domestic Mail Manual (DMM) in effect at the time of mailing. The type font must be one of the USPS accepted and verified MLOCR readable type.

MAIL PREPARATION: All envelopes will have a printed CMS First Class Mail Postage and Fees Paid permit. The contractor is cautioned to use the permit imprint only for mailing material produced under this contract. Using the CMS address tapes as provided, the contractor is required to obtain the maximum USPS postage discounts possible in accordance with the USPS First Class mail automated mail discount structure in effect at the time of mailing**.** In compliance with USPS Mail Preparation & Sortation Regulations, all mail must be appropriately marked and supported with the documentation necessary to ensure USPS acceptance. The contractor will be responsible for payment of any additional postage resulting from a loss of a discount due to irresponsible and careless application of USPS mail preparation and sortation standards.

The contractor will be required to provide mailing under the provided CMS "G-28" permit imprint via pre-sorted "First Class Mail, U.S. Postage Paid".

All mailed copies must be sorted using the ZIP + 4 code and each Item 2 Letter must contain a delivery point barcode.

Contractor to prepare mailing to maximize presort discount and comply with USPS mailing requirement for automations compatible mailing in effect at the time of mailing. The submitted files by CMS have been CASS and NCOA certified. Contractor sponsored address data enhancements to secure postal discount **MUST NOT** negatively affect deliverability and/or omit/change any required address field as provided by CMS address files. It is the contractor's responsibility to keep up to date on all USPS requirements. Any address/mail management related questions/issues may be directed to Ray Wajbel, CMS, at (410) 786-7887, or E-mail **raymond.wajbel@cms.hhs.gov**.

All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for domestic Presorted First Class Mail, as applicable, and must be prepared for the most cost effective mailing rate/class obtainable, including ZIP + 4, bar-coding, and presorting for maximum postal automation discounts (as applicable). The placement and application of the POSTNET bar codes must not compromise any applicable USPS addressing/imprinting requirements.

Contractor may be responsible for any postage fees related to undeliverable letters caused by print quality control issues.

VERIFICATION OF PRODUCTION AND MAILING: Contractor will be responsible for validating the integrity of every notice produced in all phases of printing, inserting and mailing and to ensuring all notices received from CMS were correctly entered into the United States postal system.

A recovery system will be required to ensure that all defective or missing/mutilated pieces detected are identified, reprinted and replaced. The recovery system must use unique sequential numbers assigned to each piece to aid in the recovery and replacement of any defective or missing/mutilated pieces, and must be capable of tracking and/or locating any individual piece of mail from the time it leaves the press, up to and including when it is off-loaded at the USPS facility.

Note: The Government will not as a routine matter request that the contractor produce individual pieces in transit within the plant, however, the contractor must demonstrate that they have an audit trail established that has the ability to comply with this type request when and if the need arises.
The quality control plan must account for the number of pieces mailed daily.

The contractor shall monitor all aspects of the job including material handling and mail flow, to assure that the production and delivery of these notices meet specifications and Government requirements.

QUALITY ASSURANCE LEVELS AND STANDARDS: The following levels and standards shall apply to these specifications:

Product Quality Levels:
(a) Printing Attributes - Level 3
(b) Finishing Attributes - Level 3

Inspection Levels (from ANSI/ASQC Zl.4):
(a) Non-destructive Tests--General Inspection Level I.
(b) Destructive Tests ----- Special Inspection Level S-2.

Specified Standards--The specified standards for the attributes requiring them shall be:

Attribute	**Specified Standard**
P-7. Type Quality and Uniformity	Press Sheet/ Imaging Inspection/ Proofs
P-10. Process Color Match	Press Sheet/ Proofs

QUALITY SYSTEMS: The prime contractor shall initiate, prior to start-up and maintain throughout the life of this contract, Quality systems to assure conformance to all requirements of this contract. The Quality systems plan should address what actions will be initiated when defects are detected.

The Quality systems shall assure the quality of components from subcontractors and subsidiary plants. This element includes assuring that components from different sources will be compatible BEFORE the start of production.

The Quality systems shall include procedures for assuring that all variable date are accurately and completely printed and that all addressed items are mailed. The procedures shall explicitly describe the methods to be used to assure that no records are missed or duplicated when ant interruption of variable printing occurs (e.g. due to equipment malfunction).

Records of tests, inspections, and critical processes shall be timed stamped and maintained on file. The records must be available to GPO and or HHS employees until the expiration of the warranty period of this contract.

All quality control samples must be produced at no additional cost to the Government.

Quality Control Procedures: The contractor shall provide and maintain, within their own organization, an independent quality assurance organization of sufficient size and expertise to monitor the operations performed, and inspect the products of each operation to a degree and extent that will ensure the Government's quality assurance, inspection, and acceptance provisions herein are met. The contractor shall perform, or have performed, the process controls, inspections and tests required to substantiate that the products provided under this solicitation conform to the specifications. The contractor shall provide what actions to be taken to insure defective, missing/mutilated, or blank envelopes are removed prior to mailing. If defective, missing or mutilated pieces are discovered these pieces must be mailed as residual items. These actions must be consistent with the requirements found in GPO Contract Terms (GPO Pub. 310.2, effective December 1, 1987, Rev. 6/01).

Contractor may be responsible for any postage fees related to undeliverable letters caused by print quality control issues.

SCHEDULE: Adherence to this schedule must be maintained. See "Notice of Compliance with Schedules", in GPO Pub. 310.2. **Furnished material will be available for pick up on January 6, 2009.** Purchase Order will be available for pickup at the U.S. Government Printing Office, Columbus Regional Printing Procurement Office, Suite 112-B, 1335 Dublin Road, Columbus, OH 43215. Disk material, file transfer and envelope copy will be available at CMS, 7500 Security Blvd., Baltimore, MD 21244-1850.

Mail complete on or before January 12, 2009.

The contractor must mail completed pieces on a daily basis as production runs are completed.

The contractor must e-mail on a daily basis production and mailing counts with totals of overall complete and remaining counts to: Attn: Pat McNaughton PAtrick.McNaughton@cms.hhs.gov, Raymond Wajbel Raymond.wajbel@cms.hhs.gov and Bill Lansky wlansky@gpo.gov.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with the order or shortly thereafter. In the event such information is not received in due time, the contractor will not be relieved of any responsibility in meeting the shipping schedule because of failure to request such information.

DISTRIBUTION: Mail f.o.b. contractor's city using the provided CMS "G-28" permit imprint via pre-sorted "First Class Mail, U.S. Postage Paid". All expenses incidental to picking up and returning materials, proofs, etc. must be borne by the contractor.

The contractor is cautioned that "Postage and Fees Paid" indicia may be used only for the purpose of mailing material produced under the contract. All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for "Domestic Mail" as applicable.

The contractor will be required to submit the properly completed Postal Service form(s) (or equivalent) with the voucher for billing.

Deliver PROOFS and 20 random samples to: CMS/ Attn: Pat McNaughton (410-786-9311), Mail Stop SL-11-16, 7500 Security Blvd., Baltimore, MD 21244-1850. (Phone 410-786-9311)

MAILING STATEMENT: Contractor must complete and supply all copies of all USPS 3602's and GPO 712's to CMS within 24 hours of USPS certification. Copies must be sent to CMS, Attn: Pat McNaughton (410-786-9311), Mail Stop SL-11-16, 7500 Security Blvd., Baltimore, MD 21244-1850.

RETURN OF GOVERNMENT FURNISHED PROPERTY: The contractor must submit all material furnished by the Government along with any films made by the contractor, together with one copy of all USPS 3602's and GPO 712's within 24 hours after completions of mailing to: **CMS, Attn: Pat McNaughton (410-786-9311), Mail Stop SL-11-16, 7500 Security Blvd., Baltimore, MD 21244-1850.**

The materials must be packaged, properly labeled, and returned separate from the entire job. The contractor must be able to produce a separate signed receipt for these materials at any time during the contract.

All expenses incidental to pickup/return of materials, and furnishing sample copies must be borne by the contractor.

Attachment A

Field Name	Location	Size	Type
First name	1	20	Char
Filler	21	1	space
Middle name	22	1	char
Filler	23	1	space
Last name	24	20	char
Address Line 1	44	22	Char
Address Line 2	66	22	Char
Address Line 3	88	22	Char
Address Line 4	110	22	Char
Address Line 5	132	22	Char
Address Line 6	154	22	Char
City	176	15	Char
State	191	2	Char
ZIP Code	193	9	Num
Filler	202	9	Char (spaces)

THERE IS NO ATTACHMENT B

Attachment C

Secure One HHS

Information Security Program Rules of Behavior

The *HHS Rules of Behavior* (HHS Rules) provides common rules on the appropriate use of all HHS technology resources and information[1] for Department users, including federal employees, interns and contractors. The HHS rules work in conjunction with the *HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources*, dated February 17, 2006, and are issued under the authority of the HHS-OCIO-2007-0002, Policy for Department-wide Information Security, dated September 25, 2007. Both references may be found at URL: http://www.hhs.gov/ocio/policy/index.html.

All users of Department technology, resources, and, information must read these rules and sign the accompanying acknowledgement form before accessing Department data/information, systems and/or networks. This acknowledgement must be signed annually, preferably as part of Information Security Awareness Training, to reaffirm knowledge of and agreement to adhere to the HHS rules. The HHS rules may be presented to the user in writing or electronically, and the user's acknowledgement may be obtained by written or electronic signature. Each Operating Division (OPDIV) Chief Information Officer (CIO) shall determine how signatures are to be submitted, retained, and recorded[2]; and may append any necessary information or fields to the signature page. For electronic signatures, the specific version number of the HHS rules must be retained along with the date, and sufficient identifying information to uniquely link the signer to his or her corresponding information system accounts. Electronic copies of the signed Signature Page may be retained in lieu of the original. Each OPDIV CIO shall ensure that information system and information access is prohibited in the absence of a valid, signed HHS rules from each user.

Each HHS OPDIV may require user certification to policies and requirements, more restrictive than the rules prescribed herein, for the protection of OPDIV information and systems.

Furthermore, supplemental rules of behavior may be created for systems which require users to comply with rules beyond those contained in the HHS Rules. In such cases, users must additionally sign these supplemental rules of behavior prior to receiving access to these systems, and must comply with any ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners shall document system-specific rules of behavior and any recurring requirement to sign them in the System Security Plan for their systems. Each OPDIV CIO shall implement a process to obtain and retain the signed rules for such systems and shall ensure that user access to their information is prohibited without a signed, system-specific rules and a signed HHS Rules.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively, implement their own system-specific rules.

These HHS Rules apply to both the local and remote use of HHS information (in both electronic and physical forms) and information systems by any individual.

- Information and system use must comply with Department and OPDIV policies and standards, and with applicable laws.
- Use for other than official, assigned duties is subject to the HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources, dated February 17, 2006.
- Unauthorized access to information or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII)[3]

Users shall:

- In accordance with OPDIV procedures, immediately report all lost or stolen HHS equipment, known or suspected security incidents, known or suspected information security policy violations or compromises, or suspicious activity. Known or suspected security incidents is inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including PII, maintained or in possession of the OPDIV.
- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on Departmental systems.
- Wear identification badges at all times in federal facilities.
- Log-off or lock systems when leaving them unattended.
- Use provisions for access restrictions and unique identification to information and avoid sharing accounts.
- Complete security awareness training before accessing any HHS/OPDIV system and on an annual basis thereafter. Also, complete any specialized role-based security or privacy training, as required. See Memo from HHS CIO: Training of Individuals Developing and Managing Sensitive Systems, dated November 7, 2007.
- Permit only authorized HHS users to use HHS equipment and/or software.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with HHS records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information necessary to perform job functions (i.e., need to know).
- Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published system of records notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary, to assure fairness in making determinations about an individual.

Users shall **not**:

- Direct or encourage others to violate HHS policies.
- Circumvent security safeguards or reconfigure systems except as authorized (i.e., violation of least privilege).
- Use another person's account, identity, or password.
- Remove computers or equipment.
- Send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums.
- Exceed authorized access to sensitive information.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on portable devices such as laptops, personal digital assistants (PDA) and universal serial bus (USB) drives or on remote/home systems without authorization or appropriate safeguards, as stipulated by the HHS Encryption Standard for Mobile Devices and Portable Media, dated August 21, 2007.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others. (See 18 U.S.C. 2071)
- Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without permission or license from the copyright owner.
- Modify software without management approval.

The following are prohibited on Government systems per the HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources, dated February 17, 2006:

- Sending or posting obscene or offensive material in messages or forums.
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages.
- Sending messages supporting political activity restricted under the Hatch Act.
- Conducting any commercial or "for-profit" activity.
- Utilizing peer-to-peer software without OPDIV CIO approval.
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material.
- Operating unapproved web sites.
- Incurring more than minimal additional expense, such as using non-trivial amounts of storage space or bandwidth for personal files or photos.
- Using the Internet or HHS workstation to play games, visit chat rooms, or gamble.

Users shall ensure the following protections are properly engaged, particularly on non-HHS equipment or equipment housed outside of HHS facilities:

- Use antivirus software with the latest updates.
- On personally-owned systems, use of anti-spyware and personal firewalls.
- For remote access and mobile devices, a time-out function that requires re-authentication after no more than 30 minutes of inactivity.
- Adequate control of physical access to areas containing sensitive information.
- Use of approved encryption to protect sensitive information stored on portable devices or recordable media, including laptops, thumb drives, and external disks; stored on remote or home systems; or transmitted or downloaded via e-mail or remote connections.
- Use of two-factor authentication for remote access to sensitive information.

Users shall ensure that passwords:

- Contain a minimum of eight alphanumeric characters and (when supported by the OPDIV environment) at least one uppercase and one lowercase letter, and one number, and one special character.
- Avoid words found in a dictionary, names, and personal data (e.g., birth dates, addresses, social security numbers, and phone numbers).
- Are changed at least every 90 days, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords).
- Are not reused until at least six other passwords have been used.
- Are committed to memory, or stored in a secure place.

SIGNATURE PAGE

I have read the *HHS Rules of Behavior* (HHS Rules), version 2008-0001.003S, dated February 12, 2008 and understand and agree to comply with its provisions. I understand that violations of the HHS Rules or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities. I understand that exceptions to the HHS Rules must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS Rules draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Signatures: _____

Date Signed: _____

Employee's/User's Name: _____

(Print)

APPROVED BY AND EFFECTIVE ON:

/s/ February 12, 2008

Michael Carleton
HHS Chief Information Officer

DATE

The record copy is maintained in accordance with GRS 1, 18.a.

Attachment D

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

INSTRUCTIONS FOR COMPLETING THE DATA USE AGREEMENT (DUA) FORM CMS-R-0235

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

This agreement must be executed prior to the disclosure of data from CMS' Systems of Records to ensure that the disclosure will comply with the requirements of the Privacy Act, the Privacy Rule and CMS data release policies. It must be completed prior to the release of, or access to, specified data files containing protected health information and individual identifiers.

Directions for the completion of the agreement follow:

Before completing the DUA, please note the language contained in this agreement cannot be altered in any form.

- First paragraph, enter the Requestor's Organization Name.
- Section #1, enter the Requestor's Organization Name.
- Section #4 enter the Study and/or Project Name and CMS contract number if applicable for which the file(s) will be used.
- Section #5 should delineate the files and years the Requestor is requesting. Specific file names should be completed. If these are unknown, you may contact a CMS representative to obtain the correct names The System of Record (SOR) should be completed by the CMS contact or Project Officer. The SOR is the source system the data came from.
- Section #6, complete by entering the Study/Project's anticipated date of completion.
- Section #12 will be completed by the User.
- Section #16 is to be completed by Requestor.
- Section #17, enter the Custodian Name, Company/Organization, Address, Phone Number (including area code), and E-Mail Address (if applicable). The Custodian of files is defined as that person who will have actual possession of and responsibility for the data files. **This section should be completed even if the Custodian and Requestor are the same.** This section will be completed by Custodian.
- Section #18 will be completed by a CMS representative.
- Section #19 should be completed if your study is funded by one or more other Federal Agencies. The Federal Agency name (other than CMS) should be entered in the blank. The Federal Project Officer should complete and sign the remaining portions of this section. If this does not apply, leave blank.
- Sections #20a AND 20b will be completed by a CMS representative.
- Addendum, CMS-R-0235A, should be completed when additional custodians outside the requesting organization will be accessing CMS identifiable data.

Once the DUA is received and reviewed for privacy and policy issues, a completed and signed copy will be sent to the Requestor and CMS Project Officer, if applicable, for their files.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approved
OMB No. 0938-0734

DATA USE AGREEMENT

DUA #

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

CMS agrees to provide the User with data that reside in a CMS Privacy Act System of Records as identified in this Agreement. In exchange, the User agrees to pay any applicable fees; the User agrees to use the data only for purposes that support the User's study, research or project referenced in this Agreement, which has been determined by CMS to provide assistance to CMS in monitoring, managing and improving the Medicare and Medicaid programs or the services provided to beneficiaries; and the User agrees to ensure the integrity, security, and confidentiality of the data by complying with the terms of this Agreement and applicable law, including the Privacy Act and the Health Insurance Portability and Accountability Act. In order to secure data that reside in a CMS Privacy Act System of Records; in order to ensure the integrity, security, and confidentiality of information maintained by the CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and _____ *(Requestor)* _____ enter into this agreement to comply with the following specific paragraphs.

1. This Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the U.S. Department of Health and Human Services (HHS), and _____ *(Requestor)* _____, hereinafter termed "User."

2. This Agreement addresses the conditions under which CMS will disclose and the User will obtain, use, reuse and disclose the CMS data file(s) specified in section 5 and/or any derivative file(s) that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals. This Agreement supersedes any and all agreements between the parties with respect to the use of data from the files specified in section 5 and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the Department of Health and Human Services or any of its components with respect to the data specified herein. Further, the terms of this Agreement can be changed only by a written modification to this Agreement or by the parties adopting a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the CMS point-of-contact or the CMS signatory to this Agreement shown in section 20.

3. The parties mutually agree that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS.

4. The User represents, and in furnishing the data file(s) specified in section 5 CMS relies upon such representation, that such data file(s) will be used solely for the following purpose(s).

Name of Study/Project

Produce and mail Personal Health Records Mailer

CMS Contract No. *(If applicable)*

The User represents further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plans, that have been approved by CMS or other appropriate entity as CMS may determine, represent the total use(s) to which the data file(s) specified in section 5 will be put.

The User agrees not to disclose, use or reuse the data covered by this agreement except as specified in an Attachment to this Agreement or except as CMS shall authorize in writing or as otherwise required by law, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement. The User affirms that the requested data is the minimum necessary to achieve the purposes stated in this section. The User agrees that, within the User organization and the organizations of its agents, access to the data covered by this Agreement shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purpose stated in this section (i.e., individual's access to the data will be on a need-to-know basis).

5. The following CMS data file(s) is/are covered under this Agreement.

File	Years(s)	System of Record
Personal Health Records Mailer	2009	EDB
(latest updated form to be e-mailed)		

6. The parties mutually agree that the aforesaid file(s) (and/or any derivative file(s)) including those files that directly identify individuals and those that can be used in concert with other information to identify individuals may be retained by the User until, Date 03/31/2009 hereinafter known as the "Retention Date." The User agrees to notify CMS within 30 days of the completion of the purpose specified in section 4 if the purpose is completed before the aforementioned retention date. Upon such notice or retention date, whichever occurs sooner, the User agrees to destroy such data. The User agrees to destroy and send written certification of the destruction of the files to CMS within 30 days. The User agrees not to retain CMS files or any parts thereof, after the aforementioned file(s) are destroyed unless the appropriate Systems Manager or the person designated in section 20 of this Agreement grants written authorization. The User acknowledges that the date is not contingent upon action by CMS.

   The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon notice of termination by User, CMS will cease releasing data from the file(s) to the User under this Agreement and will notify the User to destroy such data file(s). Sections 3, 4, 6, 8, 9, 10, 11, 13, 14 and 15 shall survive termination of this Agreement.

7. The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it.The safeguards shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (**http://www.whitehouse.gov/omb/circulars/a130/a130.html**) as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" (**http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf**); and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" (**http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf**). The User acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable or deducible information derived from the file(s) specified in section 5 is prohibited. Further, the User agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in section 17 without written approval from CMS unless such movement, transmission or disclosure is required by a law.

8. The User agrees to grant access to the data to the authorized representatives of CMS or DHHS Office of the Inspector General at the site indicated in section 17 for the purpose of inspecting to confirm compliance with the terms of this agreement.

9. The User agrees not to disclose direct findings, listings, or information derived from the file(s) specified in section 5, with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, but are not limited to geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death.

   The User agrees that any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the files specified in section 5 or any data derived from such files) must adhere to CMS' current cell size suppression policy. This policy stipulates that no cell (eg. admittances, discharges, patients) less than 11 may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell less than 11. By signing this Agreement you hereby agree to abide by these rules and, therefore, will not be required to submit any written documents for CMS review. If you are unsure if you meet the above criteria, you may submit your written products for CMS review. CMS agrees to make a determination about approval and to notify the user within 4 to 6 weeks after receipt of findings. CMS may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual beneficiaries

10. The User agrees that, absent express written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement to do so, the User shall not attempt to link records included in the file(s) specified in section 5 to any other individually identifiable source of information. This includes attempts to link the data to other CMS data file(s). A protocol that includes the linkage of specific files that has been approved in accordance with section 4 constitutes express authorization from CMS to link files as described in the protocol.

11. The User understands and agrees that they may not reuse original or derivative data file(s) without prior written approval from the appropriate System Manager or the person designated in section 20 of this Agreement.

12. The parties mutually agree that the following specified Attachments are part of this Agreement:

    _____

13. The User agrees that in the event CMS determines or has a reasonable belief that the User has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this Agreement or another written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement, CMS, at its sole discretion, may require the User to: (a) promptly investigate and report to CMS the User's determinations regarding any alleged or actual unauthorized use, reuse or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by CMS, submit a formal response to an allegation of unauthorized use, reuse or disclosure; (d) if requested by CMS, submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and (e) if requested by CMS, return data files to CMS or destroy the data files it received from CMS under this agreement. The User understands that as a result of CMS's determination or reasonable belief that unauthorized uses, reuses or disclosures have taken place, CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

    The User agrees to report any breach of personally identifiable information (PII) from the CMS data file(s), loss of these data or disclosure to any unauthorized persons to the CMS Action Desk by telephone at (410) 786-2850 or by e-mail notification at **cms_it_service_desk@cms.hhs.gov** within one hour and to cooperate fully in the federal security incident process. While CMS retains all ownership rights to the data file(s), as outlined above, the User shall bear the cost and liability for any breaches of PII from the data file(s) while they are entrusted to the User. Furthermore, if CMS determines that the risk of harm requires notification of affected individual persons of the security breach and/or other remedies, the User agrees to carry out these remedies without cost to CMS.

14. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i) (3)) may apply if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found to have violated sec. (i)(3) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than 10 years, or both; but if the value of such property does not exceed the sum of $1,000, they shall be fined under Title 18 or imprisoned not more than 1 year, or both.
15. By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement and acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Agreement.
16. On behalf of the User the undersigned individual hereby attests that he or she is authorized to legally bind the User to the terms this Agreement and agrees to all the terms specified herein.

Name and Title of User *(typed or printed)*		
Company/Organization		
Street Address		
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
Signature	Date	

17. The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and will be the person responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The User agrees to notify CMS within fifteen (15) days of any change of custodianship. The parties mutually agree that CMS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

    The Custodian hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User, and agrees to comply with all of the provisions of this Agreement on behalf of the User.

Name of Custodian *(typed or printed)*		
Company/Organization		
Street Address		
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
Signature	Date	

18. The disclosure provision(s) that allows the discretionary release of CMS data for the purpose(s) stated in section 4 follow(s). (To be completed by CMS staff.) _____

19. On behalf of _____ the undersigned individual hereby acknowledges that the aforesaid Federal agency sponsors or otherwise supports the User's request for and use of CMS data, agrees to support CMS in ensuring that the User maintains and uses CMS's data in accordance with the terms of this Agreement, and agrees further to make no statement to the User concerning the interpretation of the terms of this Agreement and to refer all questions of such interpretation or compliance with the terms of this Agreement to the CMS official named in section 20 (or to his or her successor).

Typed or Printed Name	Title of Federal Representative
Signature	Date
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*

20. The parties mutually agree that the following named individual will be designated as point-of-contact for the Agreement on behalf of CMS.

    On behalf of CMS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Name of CMS Representative *(typed or printed)*		
Title/Component		
Street Address		Mail Stop
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
A. Signature of CMS Representative		Date
B. Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date
Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date
Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date

Exhibit E

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

EUA WorkFlow Request No.

APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS

1. TYPE OF REQUEST *(Check only one)*:

- ❑ NEW *(Issue a CMS UserID)*
- ❑ CONNECT/DISCONNECT *(Add/remove access authorities)*
- ❑ CERTIFY *(Due date: ____/____ mo yr)*
- ❑ CHANGE USER INFORMATION *(Note new info)*
- ❑ DELETE *(Remove CMS UserID from all CMS systems)*

USERID *(Capital Letters)*

2. USER INFORMATION

- ❑ CMS Employee
- ❑ Medicare Advantage / Medicare Advantage with Prescription Drug / Prescription Drug Plan / Cost Contracts – Using HPMS Only
- ❑ Medicare Advantage / Medicare Advantage with Prescription Drug / Prescription Drug Plan / Cost Contracts – Using Other Systems
- ❑ CITIC Contractor
- ❑ Program Safeguard Contractor
- ❑ Medicare Contractor/Intermediary/Carrier
- ❑ Contractor (non-Medicare contract with CMS)
- ❑ Researcher
- ❑ Quality Improvement Organization
- ❑ End-Stage Renal Disease Network
- ❑ State Agency (State of _____)
- ❑ Federal Govt – Baltimore HR Center
- ❑ Federal Govt – Centers for Disease Control & Prevention
- ❑ Federal Govt – Commission Corps
- ❑ Federal Govt – Dept of Health & Human Services
- ❑ Federal Govt – HHS – OMHA
- ❑ Federal Govt – Dept of Justice
- ❑ Federal Govt – Dept of Veterans Affairs
- ❑ Federal Govt – Government Accountability Office
- ❑ Federal Govt – General Services Administration
- ❑ Federal Govt – Internal Revenue Service
- ❑ Federal Govt – Office of General Counsel
- ❑ Federal Govt – Office of Inspector General
- ❑ Federal Govt – Railroad Retirement Board
- ❑ Federal Govt – Social Security Administration
- ❑ Federal Govt – Other: _____
- ❑ Other: _____

First Name *(As you want it published)*	MI	Last Name *(As you want it published)*

Company/Organization/Department Name

Mailing Address *(Include Suite/Mailstop)*

City	State	ZIP Code

Office Telephone *(Include Extension)*	Company Telephone *(If different)*	E-Mail Address

IF CMS EMPLOYEE Org Name/Admin Code

Are you a Manager? ❑ Yes ❑ No

IF ONSITE AT CMS LOCATION CMS Region/Facility (Check One)

- ❑ R4 (AFC) Atlanta
- ❑ R10 (BLNCH) Seattle
- ❑ CO (CENTRAL) Central Office
- ❑ R5 (CHIICB) Chicago
- ❑ DC (COHEN) DC
- ❑ R6 (DAL1301) Dallas
- ❑ R8 (DENCSB) Denver
- ❑ R7 (FOBKAN) Kansas City
- ❑ DC (HHH) DC
- ❑ R9 (HWTHRN) San Francisco
- ❑ R1 (JFKBOS) Boston
- ❑ R2 (JKJNYC) New York
- ❑ CO (LBDCO) Central Office
- ❑ CO (NORTH) Central Office
- ❑ R3 (PHIPLB) Philadelphia
- ❑ CO (SOUTH) Central Office
- ❑ Other _____

Mail Stop	Desk Location

Form CMS-20037 (09/05) EF 09/2005

3. WORKLOAD INFORMATION

Contract Number(s) *(for Medicare Advantage/Medicare Advantage with Prescription Drug/Prescription Drug Plan/Cost Contracts — Hxxxx, Sxxxx, etc.)*

Carrier Number(s) *(for Medicare Contractors/Intermediaries/Carriers — 12345)*

Contract and Task Number *(for Contractors — CMS-05-0001 : 0001)*

Grant Number *(for Researchers)*

Inter-Agency Agreement Number

4. REQUIRED ACCESSES *(See http://www.cms.hhs.gov/mdcn/bmcjcreport.asp for list of available jobcodes)*

❑ Connect	❑ Disconnect	❑ Keep	Default CMS Employee (standard desktop & network with CMS e-mail acct)	❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	Default Non-CMS Employee (standard network access)	❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____

5. JUSTIFICATION *(If name change, show Old Name =, New Name =)*

6. APPROVALS: *(See http://www.cms.hhs.gov/mdcn/reqsigchart.pdf for approval info)*

PROVIDE SIGNATURES BELOW OR APPROVE ONLINE EUA WORKFLOW REQUEST NUMBER REFERENCED ON PAGE 1.

Authorization: We acknowledge that our Organization is responsible for all resources to be used by the person identified above and that requested accesses are required to perform their duties. We have reviewed and verified the workload information supplied is accurate and appropriate. We understand that any change in employment status or access needs are to be reported immediately via submittal of this form or EUA WorkFlow request.

1st APPROVER *(CMS Project Officer, CMS Contact, CMS Supervisor, MCIC Contact, etc.)*

Printed Name		Telephone Number
CMS UserID	Signature	Date

2nd APPROVER *(Not required for CMS employees, BHRC or Commissioned Corps)*

Printed Name		Telephone Number
CMS UserID	Signature	Date

APPLICANT: Read, complete and sign next page.

EUA WorkFlow Request No.

APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS

Printed Name *(As you want it published)*

Social Security Number

CMS USERID

PRIVACY ACT STATEMENT

The information on page 1 of this form is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10) (The Privacy Act of 1974). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnish on this form will be maintained in the Individuals Authorized Access to the Centers for Medicare & Medicaid Services (CMS) Data Center Systems of Records and may be disclosed as a routine use disclosure under the routine uses established for this system as published at 59 FED.REG.41329 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

The Social Security Number (SSN) is used as an identifier in the Federal Service because of the large number of present and former Federal employees and applicants whose identity can only be distinguished by use of the SSN. Collection of the SSN is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary. However, if you do not provide this information, you will not be granted access to CMS computer systems.

SECURITY REQUIREMENTS FOR USERS OF CMS COMPUTER SYSTEMS

CMS uses computer systems that contain sensitive information to carry out its mission. Sensitive information is any information, which the loss, misuse, or unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine reviews for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your IDENTIFICATION NUMBER AND/OR PASSWORD to someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions.
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to your component's Information Systems Security Officer.

Applicant's Signature	Date

Exhibit F

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (NON-CMS ONLY)

Date

PART I — TO BE COMPLETED BY REQUESTOR *(Please type or print)*

Social Security Number

Phone Number *(include extension)*

Applicant's Name *(Print Clearly)* *(Last)* *(First)* *(Middle)*

Contract Company Name *(if subcontractor, include parent company)*

PART II — REASON FOR APPLICATION *(Required)*

Reason:

- ☐ Change in job requirements
- ☐ Renewal
- ☐ Initial Issuance
- ☐ Replacement due to loss
- ☐ Name change from *(Print former name below)*:

PART III — TYPE OF BADGE *(Required for initial issuance only)*

Type:

- ☐ Contractor
- ☐ Security
- ☐ Former HCFA/CMS Employee *(Ethics Officer Signature required)*

PART IV — ELECTRONIC ACCESS *(required for all accesses to CMS secured areas)* (Pin # Selection - Pin # *(4 digit)*

ELECTRONIC ACCESSES *(check all accesses needed to perform duties)*:

- ☐ CMS Data Center
- ☐ Voice Data Switch
- ☐ LBD ADP Room
- ☐ ITF Room
- ☐ Mailroom
- ☐ LBD Voice Room
- ☐ Secure Server
- ☐ ASG Siteman
- ☐ Gov. Court
- ☐ CDC Warehouse
- ☐ 'S' Sign-in Authority *(*see bold statement in Privacy Act on reverse side)*

☐ ADP Satellite Room(s) — *(specify room numbers)*

PART V — ELECTRONIC ACCESS JUSTIFICATION
(Required for all accesses requested in PART IV)

Electronic Access Justification

PART VI — PROPERTY PASS INFORMATION

Property Description
1
2

Property Serial No.
1
2

OOM/SSS Authorization

PART VII — BACKGROUND INVESTIGATION

- ☐ Non-Sensitive **LEVEL 1**
- ☐ Public Trust **LEVEL 5**
- ☐ Public Trust **LEVEL 6**

PART VIII — AUTHORIZATIONS *(required)*

Project Officer – *(Print name clearly)* Phone Number

Project Officer - Signature Date

Note: You are required to collect Government issued ID and/or Access Card(s) at end of Contractor's project.

Contract Officer – *(Print name clearly)* Phone Number

Contract Officer – Signature Date

Contract Number

Contract Expiration Date

Form CMS-730A (11/03) (ALL OTHER EDITIONS OBSOLETE)

PRIVACY ACT ADVISORY STATEMENT

As required by 5 U.S.C. 552a (The Privacy Act of 1974 and Executive Order No.9397), you are advised that the Centers for Medicare & Medicaid Services (CMS) is authorized to collect the data on this form by 63 Stat. 390, 40 U.S.C. 86(c), and 41 C.F.R. 101-20.111. Your response to the questions on this form is not required by law. However, if you do not provide this information, your application for privileges may be denied or delayed in processing. No disclosure of this information will be made unless required by law or with written consent.

The information on side 1 of this form is collected and maintained under the authority of 41 CFR 101-20.302, "Conduct on Federal Property" and "OMB Circular A-123, Internal Control Systems." This information is used for assigning, controlling, tracking and reporting permanently or temporarily issued unescorted access into a Government Facility. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances. Public Law 93-579, the Privacy Act of 1974, provides penalties of up to $5,000 for willful disclosure of material in any manner to any person or agency not entitled to protected information, which includes the utilization of your badge to sign-in individuals or groups which you do not escort throughout the complex. ***Your signature authorizing admittance to anyone into any CMS facility means that you are responsible for the whereabouts and conduct of said person(s). Please be advised that all persons being signed in to the CMS facilities are considered visitors. ONLY Visitor badges will be issued. If any visitor is found unescorted within the complex, they may be escorted off the premises. By signing below you acknowledge and accept these requirements necessary for this privilege. If you are found to be in violation of any of these requirements, this privilege may be revoked.**

The information you furnish on this form will be maintained in the Records of Individuals Issued Card Key System (RICKS) and the CMS Employee Pass File (EMPASS) Systems of Record and may be disclosed as a routine use disclosure under those uses established for this system as published in the Federal Register and as CMS may establish in the future by publication in the Federal Register.

By signing below you accept the responsibility of being issued an official Civilian Government Employee Identification Badge. This includes immediate notification to the security office if your badge is lost or stolen.

All CMS Government issued identification, access cards, and parking permits must be returned to the ASG, Security and Safety Staff prior to the last day of employment at CMS, or expiration of authorized access. Individuals who do not return their Government issued Access card(s) within 48 hours following separation from CMS (regardless of contract date), will be permanently barred from the CMS complex and are subject to fines and penalties associated with theft of Government property under Federal Property Management Regulations, Title 41, Code of Federal Regulations, Preservation of Property Subpart 101-20.303.

_____ _____

Signature Date

REQUIRED APPROVALS

OIS / OOM Use Only

CARD NO._____

OIS/TMG Physical Security Officer for Computer Facilities _____

OOM/SSS Personnel Security Representative _____

Background Investigation Conducted ☐ Level 1 ☐ Level 5 ☐ Level 6

OOM/SSS Badging Personnel Initials _____

INSTRUCTIONS: REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES

Prior to submitting form CMS-730A to the Security and Safety Staff, ASG, OOM (SLL-11-05), ALL required signatures MUST be obtained, otherwise this form will not be processed. NO EXCEPTIONS.

All forms, requiring electronic access to any CMS facility, must be submitted to the OIS/TMG Physical Security Officer for Computer Facilities (m/s N1-19-18 — desk N1-24-17).

NOTE: Each time a CMS-730A form is revised it supersedes the previous form. You must enter all accesses needed.

Purpose of this Form

Information from this form is used primarily as the basis to grant access to any CMS facility and secured areas.

Part I – Applicant Information *(To be completed by Applicant – Required):*

SSN – Provide SSN
Phone Number – Provide the phone number where you can be contacted during duty hours.
Applicant's Name – Print full name clearly.
Company Name – Print company name *(clearly – if subcontractor, please include parent company name).*

Part II – Reason For Application (*Required):*

Check the reason for this application.

Part III – Type of Badge *(required for initial issuance only)*:

Enter type of badge needed.

PART IV – Electronic Access *(Required for access to secured areas)*:

Be sure to select a personal 4-digit pin number in the space provided.

Electronic Access areas *(secured areas)* should only be requested if you need them to perform your duties. A thorough justification is mandatory for anyone requesting electronic access (PART V).

PART V – Electronic Access Justification *(Required for all accesses checked in PART IV)*

A thorough justification is required for all accesses requested in PART IV. Just stating access is needed will not be accepted as a justification.

PART VI – Property Pass Information:

Provide a description and serial number for each item you are bringing into the building.

PART VII – Background Investigation:

Provide a level of investigation that corresponds to your job duties/responsibilities *(position sensitivity determination).*

PART VIII – Authorizations: *(To be completed by Project Officer)*

Project Officer's Name – Print name clearly.
Project Officer's Signature – Sign name and date. *(see Note)*

Authorizations: *(To be completed by Contract Officer)*

Contract Officer's Name – Print name clearly.
Contract Officer's Signature – Sign name and date.
Contract Number – Provide the contract number of applicant's company.
Contract Expiration Date – Provide the contract expiration date of applicant's company.

You are responsible for reading the Privacy Act Statement on Page 2 of the Request for Physical Access to CMS Facilities Form. Your signature is required, as indicated under the Privacy Act Statement, to acknowledge you have read these requirements.

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 1 of 5

CMS SPECIFIC PROVISIONS FOR ALL NEW SOLICITATIONS AND CONTRACTS:

Security Clause -Background - Investigations for Contractor Personnel

If applicable, Contractor personnel performing services for CMS under this contract, task order or delivery order shall be required to undergo a background investigation. CMS will initiate and pay for any required background investigation(s).

After contract award, the CMS Project Officer (PO) and the Security and Emergency Management Group (SEMG), with the assistance of the Contractor, shall perform a position-sensitivity analysis based on the duties contractor personnel shall perform on the contract, task order or delivery order. The results of the position-sensitivity analysis will determine first, whether the provisions of this clause are applicable to the contract and second, if applicable, determine each position's sensitivity level (i.e., high risk, moderate risk or low risk) and dictate the appropriate level of background investigation to be processed. Investigative packages may contain the following forms:

1. SF-85, Questionnaire for Non-Sensitive Positions, 09/1995
2. SF-85P, Questionnaire for Public Trust Positions, 09/1995
3. OF-612, Optional Application for Federal Employment, 12/2002
4. OF-306, Declaration for Federal Employment, 01/2001
5. Credit Report Release Form
6. FD-258, Fingerprint Card, 5/99, and
7. CMS-730A, Request for Physical Access to CMS Facilities (NON-CMS ONLY), 11/2003.

The Contractor personnel shall be required to undergo a background investigation commensurate with one of these position-sensitivity levels:

1) High Risk (Level 6)
Public Trust positions that would have a potential for exceptionally serious impact on the integrity and efficiency of the service. This would include computer security of a major automated information system (AIS). This includes positions in which the incumbent's actions or inaction could diminish public confidence in the integrity, efficiency, or effectiveness of assigned government activities, whether or not actual damage occurs, particularly if duties are especially critical to the agency or program mission with a broad scope of responsibility and authority.

Major responsibilities that would require this level include:

a. development and administration of CMS computer security programs, including direction and control of risk analysis and/or threat assessment;

b. significant involvement in mission-critical systems;
c. preparation or approval of data for input into a system which does not necessarily involve personal access to the system but with relatively high risk of causing grave damage or realizing significant personal gain;
d. other responsibilities that involve relatively high risk of causing damage or realizing personal gain;
e. policy implementation;
f. higher level management duties/assignments or major program responsibility; or
g. independent spokespersons or non-management position with authority for independent action.

2) Moderate Risk (Level 5)
Level 5 Public Trust positions include those involving policymaking, major program responsibility, and law enforcement duties that are associated with a "Moderate Risk." Also included are those positions involving access to or control of unclassified sensitive, proprietary information, or financial records, and those with similar duties through which the incumbent can realize a significant personal gain or cause serious damage to the program or Department. Responsibilities that would require this level include:

a. the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the High Risk level to ensure the integrity of the system;
b. systems design, operation, testing, maintenance, and/or monitoring that are carried out under the technical review of a higher authority at the High Risk level;
c. access to and/or processing of information requiring protection under the Privacy Act of 1974;
d. assists in policy development and implementation;
e. mid-level management duties/assignments;
f. any position with responsibility for independent or semi-independent action; or
g. delivery of service positions that demand public confidence or trust.

3) Low Risk (Level 1)
Positions having the potential for limited interaction with the agency or program mission, so the potential for impact on the integrity and efficiency of the service is small. This includes computer security impact on AIS.

The Contractor shall submit the investigative package(s) to SEMG within three (3) days after being advised by the SEMG of the need to submit packages. Investigative packages shall be submitted to the following address:

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 3 of 5

Centers for Medicare & Medicaid Services
Office of Operations Management
Security and Emergency Management Group
Mail Stop SL-13-15
7500 Security Boulevard
Baltimore, Maryland 21244-1850

The Contractor shall submit a copy of the transmittal letter to the Contracting Officer (CO).

Contractor personnel shall submit a CMS-730A (Request for Badge) to the SEMG (see attachment in Section J). The Contractor and the PO shall obtain all necessary signatures on the CMS-730A prior to any Contractor employee arriving for fingerprinting and badge processing.

The Contractor must appoint a Security Investigation Liaison as a point of contact to resolve any issues of inaccurate or incomplete form(s). Where personal information is involved, SEMG may need to contact the contractor employee directly. The Security Investigation Liaison may be required to facilitate such contact.

SEMG will fingerprint contractor personnel and send their completed investigative package to the Office of Personnel Management (OPM). OPM will conduct the background investigation. Badges will not be provided by SEMG until acceptable finger print results are received; until then the contractor employee will be considered an escorted visitor. The Contractor remains fully responsible for ensuring contract, task order or delivery order performance pending completion of background investigations of contractor personnel.

SEMG shall provide written notification to the CO with a copy to the PO of all suitability decisions. The PO shall then notify the Contractor in writing of the approval of the Contractor's employee(s), at that time the Contractor's employee(s) will receive a permanent identification badge. Contractor personnel who the SEMG determines to be ineligible may be required to cease working on the contract immediately.

The Contractor shall report immediately in writing to SEMG with copies to the CO and the PO, any adverse information regarding any of its employees that may impact their ability to perform under this contract, task order or delivery order. Reports should be based on reliable and substantiated information, not on rumor or innuendo. The report shall include the contractor employee's name and social security number, along with the adverse information being reported.

Contractor personnel shall be provided an opportunity to explain or refute unfavorable information found in an investigation to SEMG before an adverse adjudication is made. Contractor personnel may request, in writing, a copy of their own investigative results by contacting:

Office of Personnel Management
Freedom of Information
Federal Investigations Processing Center
PO Box 618
Boyers, PA 16018-0618.

At the Agency's discretion, if an investigated contractor employee leaves the employment of the contractor, or otherwise is no longer associated with the contract, task order, or delivery order within one (1) year from the date the background investigation was initiated by CMS, then the Contractor may be required to reimburse CMS for the full cost of the investigation. The amount to be paid by the Contractor shall be due and payable when the CO submits a written letter notifying the Contractor as to the cost of the investigation. The Contractor shall pay the amount due within thirty (30) days of the date of the CO's letter by check made payable to the "United States Treasury." The Contractor shall provide a copy of the CO's letter as an attachment to the check and submit both to the Office of Financial Management at the following address:

Centers for Medicare & Medicaid Services
PO Box 7520
Baltimore, Maryland 21207

The Contractor must immediately provide written notification to SEMG (with copies to the CO and the PO) of all terminations or resignations of Contractor personnel working on this contract, task order or delivery order. The Contractor must also notify SEMG (with copies to the CO and the PO) when a Contractor's employee is no longer working on this contract, task order or delivery order.

At the conclusion of the contract, task order or delivery order and at the time when a contractor employee is no longer working on the contract, task order or delivery order due to termination or resignation, all CMS-issued parking permits, identification badges, access cards, and/or keys must be promptly returned to SEMG. Contractor personnel who do not return their government-issued parking permits, identification badges, access cards, and/or keys within 48 hours of the last day of authorized access shall be permanently barred from the CMS complex and subject to fines and penalties authorized by applicable federal and State laws.

Work Performed Outside the United States and its Territories

The contractor, and its subcontractors, shall not perform any activities under this contract at a location outside of the United States, including the transmission of data or other information outside the United States, without the prior written approval of the Contracting Officer. The factors that the Contracting Officer will consider in making a decision to authorize the performance of work outside the United States include, but are not limited to the following:

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 5 of 5

1. All contract terms regarding system security
2. All contract terms regarding the confidentiality and privacy requirements for information and data protection
3. All contract terms that are otherwise relevant, including the provisions of the statement of work
4. Corporate compliance
5. All laws and regulations applicable to the performance of work outside the United States
6. The best interest of the United States

In requesting the Contracting Officer's authorization to perform work outside the United States, the contractor must demonstrate that the performance of the work outside the United States satisfies all of the above factors. If, in the Contracting Officer's judgment, the above factors are not fully satisfied, the performance of work outside the United States will not be authorized. Any approval to employ or outsource work outside of the United States must have the concurrence of the CMS SEMG Director or designee.

GPO Jacket 540 - 253, Attachment H
FAQ Supplement to CMS Security Clause 09A-01
Date: April 4, 2008
Page 1 of 3

CMS Security Clause 09A-01 is a mandatory clause required in all CMS contracts that require background investigations. This Frequently Asked Questions (FAQ) Supplement provides additional information specific to CMS print/mail contracts.

Acronyms
CMS – Centers for Medicare & Medicaid Services, Department of Health and Human Services
OMB – Office of Management and Budget, Executive Office of the President
OPM – United States Office of Personnel Management
PO – CMS Project Officer
PS – CMS Printing Specialist
PSC -- Program Support Center, Department of Health and Human Services
PII – Personally Identifiable Information (i.e. beneficiary name and address)
PIV – Personal Identity Verification
SEMG – CMS Security & Emergency Management Group

Who must apply for and receive a background investigation?

Contractor personnel with access to CMS' beneficiary PII under this contract *may be* required to undergo a background investigation. At a minimum, the two applicants for access to the Gentran mailbox *must* undergo a background investigation anticipated to be at a Public Trust Level 5. Depending on the outcome of the Preaward Security Survey and/or discussion at the Postaward Conference, additional contractor employees and/or subcontractors may be required to undergo background investigations. It is possible that everyone with access to the data processing and production areas, including janitors and maintenance technicians, must undergo a background investigation. SEMG and the PO will make this determination at the Postaward Conference.

Will production employees working on a different production line in the same room be subject to a CMS investigation? Even if they aren't working on a CMS job?

That will be determined by SEMG and the PO at the Postaward Conference. Depending on the sensitivity of the CMS job, it may be necessary to perform a background investigation on everyone with access to all work areas that contain CMS PII during performance of this contract. However, if the production line running the CMS job has limited and controlled access from other production lines, then workers outside of this area would not be subject to a CMS investigation.

What is a Security Investigation Liaison?

The contractor must appoint a Security Investigation Liaison to handle confidential personnel issues that may arise at any point during the background investigation process, and to serve as a point of contract to the Government for background investigation issues. The Liaison's duties will include attending the Postaward Conference, submitting background applications timely, and resolving any issues of inaccurate or incomplete data supplied by background investigation applicants. Where personal information is involved, SEMG may need to contact the background investigation applicant directly. The Security Investigation Liaison may be required to facilitate such contact. It is up to the contractor to decide if this should be the same or a different person who handles technical issues.

Where may I find copies of the forms listed in CMS Security Clause 09A-01?

Forms SF-85, SF-85P, OF-612, and OF-306 can be found on: www.forms.gov . However, applicants may not actually fill out these forms. These forms are listed for the similar data to be collected through "e-QIP" an online background investigation application process; more about that later in this FAQ.

The Credit Report Release Form and the FD-258 Fingerprint Card will be provided if deemed applicable at the Postaward Conference.

Form CMS-730A is provided as an attachment to this contract, contractor may reproduce as necessary at no cost to the Government. Contractor must submit a completed CMS-730A for each background investigation applicant to the PS within 5 workdays after notification by the PS Original signatures are required on this form; therefore, photocopied signatures or fax transmission is not acceptable.

The Contractor is also required to submit a PIV Spreadsheet listing all background investigation applicants. This Microsoft Excel spreadsheet will be provided to the contractor by the PS after the Postaward Conference. The PIV Spreadsheet collects the following information for each background investigation applicant: SSN, Last Name, First Name, Middle Name, Suffix, Birth Date, City of Birth, County of Birth, Country of Birth, E-mail Address, Home Phone, Previous Federal Government Background Investigations Performed, and Contracting Firm.

Send completed forms to the PS; not to the SEMG address listed on page 3 of the attached CMS Clause-09A-01. As soon as the completed forms are prepared for shipment, the contractor must e-mail transmittal information (carrier, tracking numbers, estimated time of arrival at CMS) to the PS. Email addresses will be provided at the Postaward Conference.

What is "e-QIP"?

E-QIP is a secure internet website sponsored by OPM for submission of background investigation application information. After receipt of the properly completed CMS-730A forms and PIV spreadsheet, SEMG will notify Contractor's Security Liaison that background investigation applicants are invited to enter "e-QIP". Background investigation applicants will have a 14 calendar day window to complete the e-QIP online submission. The information requested in e-QIP is similar to Forms SF-85 and SF-85P. OMB has estimated the time to complete the e-QIP application takes an average of 120 minutes. At time of e-QIP invitation notification, SEMG will also notify the Security Liaison if paper copies of Forms OF-612 and OF-306 must also be submitted by the applicants within the same 14 day window. Potential bidders may find additional information about e-QIP on the internet at: http://www.opm.gov/e-qip/ .

Why do I have to fill out a "Request for Physical Access to CMS Facilities" form?

While it is not anticipated that any contractor personnel will need physical access to CMS property, Form CMS-730A is also used to authorize CMS to perform a background investigation and to certify receipt of Privacy Act information by the applicant. Failure to provide a completed Form CMS-730A will cause a denial of access to CMS computer systems.

Why do I have to travel to CMS Central Office for fingerprinting?

CMS prefers to process electronic fingerprints generated in CMS or PSC offices. Electronic fingerprinting services are available at no cost at the CMS Central Office in Baltimore, and for a

fee at each of the regional PSC offices. PSC offices are located in downtown Federal buildings in the following cities: Boston, New York City, Philadelphia, Atlanta, Chicago, Dallas, Kansas City, Denver, San Francisco, and Seattle. Information regarding PSC locations, hours, fees, and procedures may be obtained by emailing: security@psc.hhs.gov .

If the contractor is unable to go to the above locations for electronic fingerprints, CMS will allow the contractor to obtain ink fingerprints (non-electronic) from their local police department. **Two sets** of ink fingerprints on FD-258 hard cards must be submitted to CMS directly from the police department. CMS will supply the contractor with blank FD-258 hard cards and a self addressed, stamped Priority Mail envelope for the contractor to give the police department for return of the fingerprint cards to CMS.

At the Postaward Conference, the contractor must be prepared to discuss where fingerprints will be obtained.

A number of my employees have undergone background checks by another Federal agency. Do they have to repeat the process for CMS?

That will be decided by SEMG and the PO at the Postaward Conference. If the employee performs a duty that requires a background investigation, and they have had a background investigation successfully performed by another Federal entity within the last year, then they may not have to repeat the entire process. That employee will still have to submit a CMS-730A and be listed on a PIV spreadsheet.

What happens if I don't report terminations, resignations, or adverse information of cleared people? If I do, you are going to charge me up to $2,900 for the cost of the investigation.

The person assigned the User ID, and the contractor's company, remains responsible for all data collected via the Gentran mailbox. Failure to report terminations and resignations could result in this contract being terminated for default.

Reporting of adverse information will be investigated by SEMG and handled appropriately considering the nature of the adverse information. It is possible the User ID may be terminated immediately and the contractor may have to initiate clearance for another employee.

Is the investigation good for the entire term of the contract, including all option years?

Access to the Gentran mailbox must be renewed annually or the User ID will be revoked. The CMS-730A and PIV spreadsheet must also be submitted annually. Fingerprinting and entering data into e-QIP should only occur once unless there are changes to the employee's record that necessitate updates.

Is it possible that I can perform work outside the United States and its Territories?

No, not on contracts for CMS print/mail requirements.