Jacket: 747-942

Title: Pub 10050-LE Medicare and You 2024 LP

Agency: DHHS/CMS

Bid Opening: August 23, 2023 at 1:00 PM

Contractor Name	Bid	Terms		Discounted Total	
PA Hutchison	$106,318.00	5.0%	21 days	$101,002.10	Awarded
Advantage Mailing	$123,145.59	0.25%	20 days	$122,837.73	

BID OPENING: Bids shall be opened at 1:00 p.m., prevailing Central Standard Time (CST), on August 23, 2023 for the U.S. Government Publishing Office, Southcentral Region.

ISSUE DATE: August 17, 2023

ANY QUESTIONS BEFORE AWARD CONCERNING THESE SPECIFICATIONS, CALL (214) 767-0451, EXT. 8 (TOM BACON).

SPECIFICATIONS

U.S. Government Publishing Office (GPO)
Southcentral Region

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 Publication 310.2, effective December 1, 1987 (Rev. 01-18)) and GPO Contract Terms, Quality Assurance Through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (Rev. 09-19)).

PRODUCT: This specification is for proofing, printing, binding, packing, mailing and shipping of comb bound books, with secure handling of PII required.

TITLE: Pub. 10050-LE Medicare and You 2024 - LP

QUALITY LEVEL: III Quality Assurance Through Attributes (GPO Pub 310.1, effective May 1979 (Rev. 09-19) applies.

QUANTITY: 15,646 Books

PAGES: 320 plus covers (includes divider page). See Description.

TRIM SIZE: 8-1/2 X 11”

DESCRIPTION: Black plastic comb bound book prints head to head in 4 Color Process. Covers 1 thru 4, text and divider page print type and line matter, medium ink coverage of black, and light ink coverage in yellow as highlight to text. Close registration throughout. One divider leaf for Pages 263 and 264 (bound) prints on white index stock.

SECURITY REQUIRMENTS: Contractor must maintain 100% accountability in the accuracy of imaging and mailing of all pieces throughout run. The Contractor must ensure that there are no missing or duplicate pieces and/or pieces with mis-imaged data. The Contractor must also ensure that no defective pieces enter the mail stream.

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. PII is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (Ref.: OMB Memorandum 07-16.) Other specific examples of PII include, but are not limited to:

a. Personal identification number, such as passport number, driver's license number, taxpayer identification number, or financial account or credit card number;
b. Address information, such as street address or personal email address;
c. Personal characteristics, including photographic image (especially of face or other distinguishing

characteristic), fingerprints, handwriting, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry).

SECURITY CONTROL PLAN: The contractor shall maintain in operation, an effective security system where items by these specifications are manufactured and/or stored (awaiting distribution or disposal) to assure against theft and/or the product ordered falling into unauthorized hands.

Contractor is cautioned that no Government provided information shall be used for non- government business. Specifically, no Government information shall be used for the benefit of a third party.

The Government retains the right to conduct on-site security reviews at any time during the term of the contract.

The plan shall contain at a minimum:

(1) How Government files (data) will be secured to prevent disclosure to a third party prior to and after termination of contract;

(2) Explain how all accountable materials will be handled throughout all phases of production

(3) How the disposal of waste materials will be handled;

(4) How all applicable Government-mandated security/privacy/rules and regulations as cited in this contract shall be adhered to by the contractor.

This proposed plan is subject to review and approval by the Government and award will not be made prior to approval of same.

Addresses for Mail copies 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 Applicants Information on page 3 on the Form.

Please note that the Applicants 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.

Security Exhibits: The following exhibits A through H (See Attachment #2) contain security clauses, information, and forms:

Exhibit A: CMS Clause 11: CMS Information Security
Exhibit B: CMS Clause 09A-01 Security Clause
Exhibit C: FAQ Supplement to CMS Security Clause 09A-01
Exhibit D: HHS identification (ID) Badge Request HHS-Form 745 (5/07)
(This form is used to initiate background investigations of the two people applying for access to the Gentran mailbox. No physical access, or badge, to CMS will be granted. Applicants must complete page 1 in its entirety including the applicant signature along with the date. After completing the form, return all pages to CMS within 24 hours. This form is to be submitted prior to award and renew annually thereafter if applicable.)
Exhibit E: Application for Access to CMS Computer Systems (Form CMS-20037) (The same applicants submitting the Form-745 must complete Form CMS-20037, and submit to CMS within 24 hours via an overnight courier, prior to award and renew annually thereafter if applicable.)

Exhibit F: Data Use Agreement (DUA) (Form CMS-R-0235) (Contractor management must complete CMS-R-0235, and submit it to CMS prior to award within 24 hours.
Exhibit G: Certificate of Data Destruction (Form CMS-10252) (Contractor must complete CMS-10252 at the expiration of the DUA.)
Exhibit H: Secure One HHS, Information Security Program Rules of Behavior
NOTE: These forms are provided as attachments (PDF file). See below. A MS Word file will be sent with the GFM upon award.

All contractor management and employees involved in this contract must read and sign this document. Signed copies of this document for Gentran applicants and DUA applicants must be submitted to CMS immediately prior to award. Signed copies for all other employees will be maintained by the contractor and furnished to the Government upon request.

The contractor must submit all completed and signed security forms (original signatures only, no photocopy or facsimile signatures will be accepted) via an overnight courier to: CMS, Attn: Clint Howard SLL-11-17 (410-786-1962); 7500 Security Blvd, Baltimore, MD 21244. For delivery directly to Attn: Clint Howard SLL-11-17 (410-786-1962); the contractor is encouraged to use an overnight/express mail contractor as determined by CMS.

GOVERNMENT TO FURNISH: Adobe Acrobat file (fonts included and color mode CMYK) for print files and a MS Excel spreadsheet for the bulk shipments (See Attachment #1) will be e-mailed at time of award. A Gentran Mailbox will be setup by CMS to provide access to data files for the addresses for the self-mailer copies.

ADDITIONAL INFORMATION:
- Contractor must have the ability to edit PDF files (when furnished by the Government).
- Contractor is not to request that electronic files provided be converted to a different format. If contractor wishes to convert files to a different format, the final output must be of the same or higher quality and at no additional cost to the Government.
- The contractor is cautioned that furnished fonts are the property of the Government and/or its originator. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract.
- Identification markings such as register marks, commercial identification marks of any kind, etc., GPO imprint, form number and revision date, carried in the electronic files, must not print on the finished product.
- Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure correct output of the required reproduction image. Any errors, media damage or data corruption that might interfere with proper file image processing must be reported to your contract administrator.
- The contractor shall create/alter any necessary trapping, set proper screen angles and screen frequency, and define file output selection for the imaging device being utilized. Furnished files must be imaged as necessary to meet the assigned quality level.
- When PostScript Files are not furnished - prior to making revisions, the contractor shall copy the furnished files and make all changes to the copy.

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. 13*, dated September 2019.

Covers & Divider: JCP Code* K10, Index, White, Basis Size 25.5 X 30.5" Basis Weight 110 lb.
Text: JCP Code* A60, Uncoated Text, White, Basis Size 25 X 38" Basis Weight 60 lb.

INK: Four Color Process

MARGINS: Adequate gripper.

PROOFS: Contractor to submit one Press Quality PDF soft proof (for content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proofs will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match. Contractor must call 214-767-0451 x 8 to confirm receipt.

Email proofs on or before August 30, 2023.

The proofs will be checked for quality and compliance with these specifications, approved or approved with comments and the contractor will be notified within TWO (2) working day after receipt. If, in the opinion of the GPO and/or Department, the proofs are not a true representation of the furnished copy, or contain noticeable defects they will be rejected must be corrected and reproofed at no additional expense to the Government. The schedule stated elsewhere in these specifications CANNOT be extended to allow for such reproofing.

Email proofs to Clinton.Howard@cms.hhs.gov; contractor must also copy contract administrator at tbacon@gpo.gov. GPO jacket numbers 747-942 must appear on all correspondence.

NOTE: The day the email is sent is not the first workday of the schedule.

CONTRACTOR MUST NOT PRINT PRIOR TO RECEIVING AN "OK TO PRINT"

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

BINDING: Suitably punch along the left 11" dimension and insert black plastic combs of suitable size and capacity to ensure book lies flat when opened.

PACKING/LABELING: Mark shipping containers as follows:

Pub # 10050-LE 09-23 and ICN # 005269 on all carton labels

****Contractor must label all shipping packages with "Free Matter For The Blind". ****

Contractor must package mailed quantity, in individual mailing containers, to insure damage is not incurred during mailing and to meet all USPS postal requirements for standard mail.

Shrink film wrap suitable.

Pack NTE 40 lbs. per shipping container.

Pallets (required for motor freight shipments only): Pallets must be type III and must conform with Federal Specifications NN-P-71C, and any amendments thereto except for dimensions and single center stringer. Full entry MUST be on the 40" width. Receipt of incorrect pallets may result in a charge for each incorrect pallet which will be assessed against the contractor. This charge will cover additional costs incurred by CMS to repalletize the shipment onto correct pallets. Loaded pallets must be machine wrapped with shrinkable or stretchable plastic strong enough to retain the integrity of the pallet during transportation and handling. Do NOT use metal strapping or pallet caps for securing material on pallets. There must be no more than one partial pallet per destination.

SCHEDULE:

Award will be made and Purchase Order issued by August 25, 2023.

PDF Proofs will be due to deliver to agency and GPO on or before August 30, 2023.

INDIVIDUAL SHIPMENTS: 8,594 single copies mail f.o.b. contractor's city on or before September 29, 2023.

BULK SHIPMENTS: Contractor to deliver 7,050 books to 158 locations in various quantities from single copy to 2,500 copies from distribution list, plus 2 department copies deliver f.o.b. destination on or before October 13, 2023.

DISTRIBUTION: F.O.B. destination and F.O.B. contractor's city/origin - See Below

All expenses incidental to picking up and returning materials, and furnishing samples must be borne by the contractor. Also, refer to Articles 5 and 6, Supplemental Specifications, GPO Contract Terms, Publication 310.2, revised January 2018.

Mail FOB Contractor's City 8,594 individual copies in self-mailers using a contractor created "Free Matter for the Blind" indicia. Contractor to create mailing indicia. Ensure positioning of address/permit info is in accordance with current applicable postal regulations. Evidence of mailing must accompany the contractor's invoice for billing.

See MAIL PREPARATION and ADDRESS REQUIREMENTS below.

All shipments below are FOB Destination. INCLUDE CHARGES FOR THESE DELIVERIES IN THE QUOTED PRICE.

7,050 copies to 158 destinations. See attached distribution list (Attachment #1).

Centers for Medicare & Medicaid Services
Attn: Clint Howard SLL-11-17 (410-786-1962)
7500 Security Blvd
Baltimore, MD 21244
----- 2 books

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 fonts.

MAIL PREPARATION: It is the contractor's responsibility to keep up to date on all USPS requirements and current DMM.

Using the CMS address information as provided, the contractor is required to obtain the maximum USPS postage discounts possible. In compliance with USPS Mail Preparation & Sortation Regulations, all mail must be appropriately marked and supported with the documentation necessary to ensure USPS acceptance.

Mailing Envelopes must be prepared and sealed in a manner that will ensure acceptance, security and safe delivery by the U.S. Postal Service. Gather each piece and insert into mailing envelope, and seal. 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.

Contractor must be able to read/print up to ten lines of address information and insure all addresses can display address format acceptable for USPS automation processing. Addresses for this mailing come from a Government maintained file. For this mailing, CMS will provide certificates indicating that within 95 days the addresses have been matched against both the USPS required Coding Accuracy Support System (CASS) and National Change of Address (NCOA) software.

In the event the CASS and NCOA certification has expired, the contractor may be required to provide the certification prior to mailing. Reimbursement for this service will be made via contract modification.

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.

COMPLIANCE REPORTING: Contractor must notify the ordering agency on the same day that the product ships/delivers via e-mail to Clinton Howard (clinton.howard@cms.hhs.gov) and Tom Bacon (tbacon@gpo.gov). The subject line of this message shall be "Distribution Notice for Jacket 747-942, Req 3-00131. The notice must provide all

applicable tracking numbers, shipping method, and title. Contractor must be able to provide copies of all delivery, mailing, and shipping receipts upon agency request.

NOTIFICATION OF SHIPMENT: Immediately after the order has been shipped, the contractor MUST furnish shipping information to Agency. Include the order title, GPO jacket number, requisition number, date of shipment, quantity (copies, # of cartons, etc.), and tracking information for deliveries. Email clinton.howard@cms.hhs.gov, infosouthcentral@gpo.gov and tbacon@gpo.gov.

QUALITY ASSURANCE THROUGH ATTRIBUTES: The bidder agrees that any contract resulting from bidder's offer under these specifications shall be subject to the terms and conditions of GPO Pub. 310.1 "Quality AssuranceThrough Attributes – Contract Terms" in effect on the date of issuance of the invitation for bid. GPO Pub 310.1 is available at https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/qatap-rev-09-19.pdf

LEVELS AND STANDARDS: The following levels and standards shall apply to these specifications:
Product Quality Levels:
(a) Printing (page related) Attributes – Level III
(b) Finishing (item related) Attributes – Level III
(c) Inspection Levels (from ANSI/ASQC Z1.4):
(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	Specified Standard
P-7	Type Quality and Uniformity	Electronic Media
P-10.	Process Color Match	File Output

NOTE: Prior to award, contractor may be required to provide information related to specific equipment that will be used for production.

OFFERS: Offers must include the cost of all materials and operations for the total quantity ordered in accordance with these specifications. In addition, a price must be submitted for each additional one hundred pamphlets. The price ofthe additional quantities must be based on a continuing run, exclusive of all basic or preliminary charges (but will include shipping), and will NOT be a factor for determination of award.

BID SUBMISSION: Bidders MUST submit email bids to bidssouthcentral@gpo.gov for this solicitation. No other method of bid submission will be accepted at this time.

The Jacket number (747-942) and bid opening date (August 23, 2023) must be specified in the subject line of the emailed bid submission. Bids received after the bid opening time/date specified above will not be considered for award.

NOTE: Bidders are to fill out, sign/initial, and return pages 8-9**.**

ADDITIONAL EMAILED BID SUBMISSION PROVISIONS: The Government will not be responsible for any failure attributable to the transmission or receipt of the emailed bid including, but not limited to, the following –
1. Illegibility of bid.
2. Emails over 75 MB may not be received by GPO due to size limitations for receiving emails.
3. The bidder's email provider may have different size limitations for sending email; however, bidders are advised not to exceed GPO's stated limit.
4. When the email bid is received by GPO, it will remain unopened until the specified bid opening time. Government personnel will not validate receipt of the emailed bid prior to bid opening. GPO will use the prevailing time (specified as the local time zone) and the exact time that the email is received by GPO's email server as the official time stamp for bid receipt at the specified location.

PRE-AWARD SURVEY: In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract. As part of the financial determination, the contractor in line for award may be required to provideone or more of the following financial documents:

1) Most recent profit and loss statement
2) Most recent balance sheet
3) Statement of cash flows
4) Current official bank statement
5) Current lines of credit (with amounts available)
6) Letter of commitment from paper supplier(s)
7) Letter of commitment from any subcontractor

The documents will be reviewed to validate that adequate financial resources are available to perform the contract requirements. Documents submitted will be kept confidential, and used only for the determination of responsibility by the Government. Failure to provide the requested information in the time specified by the Government may result in the Contracting Officer not having adequate information to reach an affirmative determination of responsibility.

PAYMENT: Submitting invoices for payment via the GPO fax gateway (if no samples are required) utilizing the GPO barcode coversheet program application is the most efficient method of receiving payment. Instruction for using this method can be found at the following web address: http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

Invoices may also be mailed to: U.S. Government Publishing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401.

For more information about the billing process, refer to the General Information of the Office of Finance web page located at: https://www.gpo.gov/how-to-work-with-us/agency/billing-and-payment.

CONTRACTOR: _____

SHIPMENT(S): Shipments will be made from: City_____, State _____

The city(ies) indicated above will be used for evaluation of transportation charges when shipment f.o.b. contractor's city is specified. If no shipping point is indicated above, it will be deemed that the bidder has selected the city and state shown below in the address block, and the bid will be evaluated and the contract awarded on that basis. If shipment isnot made from evaluation point, the contractor will be responsible for any additional shipping costs incurred.

Jacket: 747-942 **Bid Price $**_____

Additional rate per 1,000 Books: _____

DISCOUNTS: Discounts are offered for payment as follows:_____Percent,_____calendar days. See Article 12 "Discounts" of Solicitation Provisions in GPO Contract Terms (Publication 310.2).

BID ACCEPTANCE PERIOD: In compliance with the above, the undersigned agree, if this bid is accepted within _____calendar days (60 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated points(s), in exact accordance with specifications.

NOTE: Failure to provide a 60-day bid acceptance period may result in expiration of the bid prior to award.

AMENDMENT(S): Bidder hereby acknowledges amendment(s) number(ed) _____

_____
(Initials)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

BIDDER'S NAME AND SIGNATURE: Unless specific written exception is taken, the bidder, by signing and submitting a bid, agrees with and accepts responsibility for all certifications and representations as required by the solicitation and GPO Contract Terms - Publication 310.2. When responding by fax or mail, fill out and return one copy of pages 8 and 9, initialing/signing where indicated.

Failure to sign the signature block below may result in the bid being declared non-responsive.

_____

(Contractor Name) (GPO Contractor's Code)

_____

(Street Address)

_____

(City – State – Zip Code)

By_____

(Printed Name, Signature, and Title of Person Authorized to Sign this Bid) (Date)

_____

(Person to be Contacted) (Telephone Number) (Email)

**********THIS SECTION FOR GPO USE ONLY**********

Certified by:_____ Contracting Officer:_____

(Initials and Date) (Initials and Date)

****

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

ATTACHMENT #1 747-942

Product Number	Name	Quantity	User Contact Name	Company Name	Address1	Address2	City	State	Zip
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Michelle Grochocinski	Wisconsin Department of Health Services	1 W Wilson St		Madison	WI	53703
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Andrea R Sneller	Region VII Area Agency on Aging	1615 S Euclid Ave		Bay City	MI	48706
10050-LE	Medicare & You 2024 (English Large Print)	1	Joseph Stone	CMS Boston Regional Office LEA	15 New Sudbury St	Rm 2325	Boston	MA	02203
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Cristina Powell	Social Security Administration	507 Jewett St	Ste B	Marshall	MN	56258
10050-LE	Medicare & You 2024 (English Large Print)	1	Christine Griffin	ServiceLink	2 Industrial Park Dr	Ste 1	Concord	NH	03301
10050-LE	Medicare & You 2024 (English Large Print)	1	Mrs. Sheron Craig	Social Security Administration	800 Centrepark Dr		Asheville	NC	28805
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Shantel J Clark	Weber Human Services	237 26th St	Rm 320	Ogden	UT	84401
10050-LE	Medicare & You 2024 (English Large Print)	1	Jenny Hubert	OCH	118 N Ozark Trl		Goodman	MO	64843
10050-LE	Medicare & You 2024 (English Large Print)	1	Mrs. Hannah Larkin-Roelse	ADRC-CW	220 3rd Ave S	Ste 1	Wisconsin Rapids	WI	54495
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Jean Horrocks	MMAP Counselor	3091 N 7th St		Onaway	MI	49765
10050-LE	Medicare & You 2024 (English Large Print)	1	Geralyn Fortney	Area Agency on Aging Pasco/Pinellas Agi	9549 Koger Blvd N	Ste 100	St Petersburg	FL	33702
10050-LE	Medicare & You 2024 (English Large Print)	1	Marlene McDaniel	SHIP	710 N Opportunity Dr		Columbia City	IN	46725
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Kari J West	The Senior Alliance	5454 Venoy Rd		Wayne	MI	48184
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Denise Joyce	Medicare Counselor	2906 Alki Ave SW		Seattle	WA	98116
10050-LE	Medicare & You 2024 (English Large Print)	1	Shelley Matson - ADRC	Aging & Disability Resource Center of Ve	402 Court House Square St		Viroqua	WI	54665
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Katrina Nesmith	Senior PharmAssist	406 Rigsbee Ave	Ste 201	Durham	NC	27701
10050-LE	Medicare & You 2024 (English Large Print)	1	David Dennie	Norfolk Public Library	235 E Plume St		Norfolk	VA	23510
10050-LE	Medicare & You 2024 (English Large Print)	1	Debi Ratliff	Rockbridge Regional Library	138 S Main St		Lexington	VA	24450
10050-LE	Medicare & You 2024 (English Large Print)	1	Judi Young	Woodbridge Human Services	4 Meetinghouse Ln		Woodbridge	CT	06525
10050-LE	Medicare & You 2024 (English Large Print)	1	Mrs. Lynn Hill	Putnam County Office for Aging	110 Old Route 6	Ste 1	Carmel	NY	10512
10050-LE	Medicare & You 2024 (English Large Print)	1	Nancy Wideman	Lutheran Senior Services	11 Hilltop Village Center Dr		Eureka	MO	63025
10050-LE	Medicare & You 2024 (English Large Print)	1	Danielle Minard	Comsewogue Public Library	170 Terryville Rd		Port Jefferson Station	NY	11776
10050-LE	Medicare & You 2024 (English Large Print)	1	Barb Wickman	Aging & Disability Resource Center of Ma	2500 Hall Ave		Marinette	WI	54143
10050-LE	Medicare & You 2024 (English Large Print)	1	Ms. Leslie Pruitt	Agency on Aging of South Central CT	117 Washington Ave	Ste 17	North Haven	CT	06473
10050-LE	Medicare & You 2024 (English Large Print)	1	Jessica Moxey	Montgomery County Health Department	11191 Illinois Route 185		Hillsboro	IL	62049
10050-LE	Medicare & You 2024 (English Large Print)	1	Mrs. Heather Noblin	Madison Senior Services	29 Bradley Rd		Madison	CT	06443
10050-LE	Medicare & You 2024 (English Large Print)	1	Rene Fannin	Green Lake County HHS/ADRC	571 County Road A		Green Lake	WI	54941
10050-LE	Medicare & You 2024 (English Large Print)	2	Mary Moran	Upper Shore Aging,Inc	403 S 7th St	Ste 127	Denton	MD	21629
10050-LE	Medicare & You 2024 (English Large Print)	2	Ms. Janet Boskill	Ks Department for Aging & Disability Srv	503 S Kansas Ave		Topeka	KS	66603
10050-LE	Medicare & You 2024 (English Large Print)	2	Mrs. Rhonda K Hunter	CMS - Atlanta	61 Forsyth Street, Suite 4-T-20		Atlanta	GA	30303
10050-LE	Medicare & You 2024 (English Large Print)	2	Mary-Ann Reeter	Lifelong	119 W Court St		Ithaca	NY	14850
10050-LE	Medicare & You 2024 (English Large Print)	2	Idaho SHIBA	Idaho Department of Insurance	700 W State St	3rd Fl	Boise	ID	83702
10050-LE	Medicare & You 2024 (English Large Print)	2	Ms. Sarah Weilacher	Franklin County Office for the Aging	355 W Main St		Malone	NY	12953

10050-LE	Medicare & You 2024 (English Large Print)	2	Ms. Angela Baker	Mount Prospect Public Library	10 S Emerson St		Mount Prospect	IL	60056
10050-LE	Medicare & You 2024 (English Large Print)	2	Mr. Sergio Trevin Verduzco	La Plata County Senior Center	2424 Main Ave		Durango	CO	81301
10050-LE	Medicare & You 2024 (English Large Print)	2	Mrs. Shalese Thomas	Prince George County Department of Famil	6420 Allentown Rd		Temple Hills	MD	20748
10050-LE	Medicare & You 2024 (English Large Print)	2	Mrs. Mary Knapp	SEKAAA	1225 130th Rd		Yates Center	KS	66783
10050-LE	Medicare & You 2024 (English Large Print)	2	Ms. Dana Thiesing	Office For The Aging	50 Sanatorium Rd	Bldg B	Pomona	NY	10970
10050-LE	Medicare & You 2024 (English Large Print)	2	Mr. Paul Benson	Social Security Adm.	252 Venture Pl		Lancaster	OH	43130
10050-LE	Medicare & You 2024 (English Large Print)	2	Ms. Crystal Behanna	Graham County Health Dept	225 N Pomeroy Ave		Hill City	KS	67642
10050-LE	Medicare & You 2024 (English Large Print)	2	Hanna Hall	Warren Hamilton Counties Office for the	1340 State Route 9		Lake George	NY	12845
10050-LE	Medicare & You 2024 (English Large Print)	2	Stefan Goslawski	Apprise	4422 Walbert Ave		Allentown	PA	18104
10050-LE	Medicare & You 2024 (English Large Print)	3	Mrs. Karen Wood	Diakon Community Services for Seniors	2020 W Norwegian St		Pottsville	PA	17901
10050-LE	Medicare & You 2024 (English Large Print)	3	Ronald Fitzgerald Moore	Centers for Medicare and Medicaid Servic	701 5th Ave	Ste 1700	Seattle	WA	98104
10050-LE	Medicare & You 2024 (English Large Print)	3	Aging Resource Center	Aging and Disablity Resorce Center	206 Court St		Chilton	WI	53014
10050-LE	Medicare & You 2024 (English Large Print)	3	Rebekah Greenwood	NWCO Medicare SHIP	775 Yampa Ave		Craig	CO	81625
10050-LE	Medicare & You 2024 (English Large Print)	3	Ms. Mary Kempf	ADRC	650 Forest Ave		Sheboygan Falls	WI	53085
10050-LE	Medicare & You 2024 (English Large Print)	4	Caitlin Milleer	HICAP-IE	2280 Market St	Ste 140	Riverside	CA	92501
10050-LE	Medicare & You 2024 (English Large Print)	4	Mrs. Sandy Bishop	Marshall County Council on Aging	436 Blount Ave		Guntersville	AL	35976
10050-LE	Medicare & You 2024 (English Large Print)	5	Brian Other (Specify) Hollins	Challenges, Options in Aging	2706 Mercer Rd		New Castle	PA	16105
10050-LE	Medicare & You 2024 (English Large Print)	5	AMY EGGLETON	Social Security Administration	1840 Jake Alexander Blvd W		Salisbury	NC	28147
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Janet Vandeusen	Legal Assistance for Seniors	333 Hegenberger Rd	Ste 850	Oakland	CA	94621
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Jo Escue	SHIP	613 College Street Rd		Elizabethtown	KY	42701
10050-LE	Medicare & You 2024 (English Large Print)	5	Pocatello SHIBA	Idaho Department of Insurance	353 N 4th Ave	Ste 200	Pocatello	ID	83201
10050-LE	Medicare & You 2024 (English Large Print)	5	Mr. Michael L Dawkins	NC DOI SHIIP	325 N Salisbury St		Raleigh	NC	27603
10050-LE	Medicare & You 2024 (English Large Print)	5	Susan B Hackney	United Way Area Agency on Aging	3600 8th Ave S		Birmingham	AL	35222
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Antoinette Gardner	GA SHIP	761 Wheaton St		Savannah	GA	31401
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Kathryn Lopan	State of Nevada SHIP/SMP/MIPPA	3320 W Sahara Ave	Ste 100	Las Vegas	NV	89102
10050-LE	Medicare & You 2024 (English Large Print)	5	Terri Esselman	Clark County ADRC	517 Court St	Rm 201	Neillsville	WI	54456
10050-LE	Medicare & You 2024 (English Large Print)	5	Emma Borck	ADRC of Jefferson County	1541 Annex Rd		Jefferson	WI	53549
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Michelle Robinson	Mercer County Senior Center	137 W Main St		Aledo	IL	61231
10050-LE	Medicare & You 2024 (English Large Print)	5	Becky McIntyre	UP Area Agency on Aging	2501 14th Ave S		Escanaba	MI	49829
10050-LE	Medicare & You 2024 (English Large Print)	5	Andrea Dickson	Wixom Public Library	49015 Pontiac Trl		Wixom	MI	48393
10050-LE	Medicare & You 2024 (English Large Print)	5	Mary Elizabeth Taylor	Braxton County Senior Citizens Center	23 Senior Center Dr		Sutton	WV	26601
10050-LE	Medicare & You 2024 (English Large Print)	5	Debbie Geiman	Country Club Tower	1515 Clubhouse Dr	4th Fl	Augusta	KS	67010
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Deborah L Wills	Hawaii County Office of Aging	74-5044 Ane Keohokalole Hwy	Bldg B	Kailua Kona	HI	96740
10050-LE	Medicare & You 2024 (English Large Print)	5	Jan Williamson	Roscommon COA	1015 Short Dr	Ste A	Prudenville	MI	48651

10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Julie Posada	Central Coast Comm for Sr Citizens	528 S Broadway		Santa Maria	CA	93454
10050-LE	Medicare & You 2024 (English Large Print)	5	Shara Bastian	Six County AOG	250 N Main St	B3	Richfield	UT	84701
10050-LE	Medicare & You 2024 (English Large Print)	5	Rachel Wright	Greene County Human Services	411 Main St	Ste 247	Catskill	NY	12414
10050-LE	Medicare & You 2024 (English Large Print)	5	Billi Charron	Princeton Senior Resource Center	101 Poor Farm Rd	Ste 2	Princeton	NJ	08540
10050-LE	Medicare & You 2024 (English Large Print)	5	Molly Sanderson	North Central-Flint Hills Area Agency on	401 Houston St		Manhattan	KS	66502
10050-LE	Medicare & You 2024 (English Large Print)	5	Mrs. Judy Crawford	Area Agency on Aging of North Texas	4309 Old Jacksboro Hwy	Ste 200	Wichita Falls	TX	76302
10050-LE	Medicare & You 2024 (English Large Print)	5	Cathy Holley	ERBA Crawford Sr. Center	300 S Lincoln St		Robinson	IL	62454
10050-LE	Medicare & You 2024 (English Large Print)	5	Ms. Jacky Robinson	Bicentennial Manor/Key Management Compan	1010 W 8th St		Junction City	KS	66441
10050-LE	Medicare & You 2024 (English Large Print)	6	Barbara Elizabeth Krueger	Deer Park Public Library	112 Front St W		Deer Park	WI	54007
10050-LE	Medicare & You 2024 (English Large Print)	6	Mr. Michael H Cober	Area Agency On Aging	240 S Wood St		Bedford	PA	15522
10050-LE	Medicare & You 2024 (English Large Print)	8	Christine Hyland	Santa Clara County Library	1370 Dell Ave	1370 Dell Ave	Campbell	CA	95008
10050-LE	Medicare & You 2024 (English Large Print)	8	Bettina Rinard	Aging and Disability Resource Center of	2600 Stewart Ave	Ste 25	Wausau	WI	54401
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. Paula Silva	Harris County Area Agency on Aging	9250 Kirby Dr		Houston	TX	77054
10050-LE	Medicare & You 2024 (English Large Print)	10	Rentha Person	AB Your Choice Insurance	5515 W Libby St		Glendale	AZ	85308
10050-LE	Medicare & You 2024 (English Large Print)	10	Ms. Toni Browning	Rappahannock Rapidan Community Services	15361 Bradford Rd		Culpeper	VA	22701
10050-LE	Medicare & You 2024 (English Large Print)	10	CDA IDAHO SHIBA	Idaho Department of Insurance	2005 N Ironwood Pkwy	Ste 143	Coeur D Alene	ID	83814
10050-LE	Medicare & You 2024 (English Large Print)	10	Alyse Bergersen	Independence Northwest	1183 New Haven Rd	Ste 4	Naugatuck	CT	06770
10050-LE	Medicare & You 2024 (English Large Print)	10	Ms. Megan Delores Gerardy	Jackson County ADRC	421 County Road R		Black River Falls	WI	54615
10050-LE	Medicare & You 2024 (English Large Print)	10	Jeanne Larson	AK SHIP	1835 Bragaw St	Ste 350	Anchorage	AK	99508
10050-LE	Medicare & You 2024 (English Large Print)	10	Loni Hitchcock	UCDD	1104 England Dr		Cookeville	TN	38501
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. Lora Bell	Tooele County Aging Services	151 N Main St	Ste 140	Tooele	UT	84074
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. Becky Faulk	Commission on Aging	1539 Sportsman Lake Rd NW		Cullman	AL	35055
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. Kimberly Haun	Swan	832 W North Ave	Ste B	Flora	IL	62839
10050-LE	Medicare & You 2024 (English Large Print)	10	Mr. George Lutz	Levittown Public Library	1 Bluegrass Ln		Levittown	NY	11756
10050-LE	Medicare & You 2024 (English Large Print)	10	Carrie Davis	Covenant Woods	7090 Covenant Woods Dr		Mechanicsville	VA	23111
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. Diane Jolly	Social Security Administration	5020 W North Ave		Milwaukee	WI	53208
10050-LE	Medicare & You 2024 (English Large Print)	10	Mr. Anthony Ruiz	Redding Rancheria Tribal Health System	2775 Bechelli Ln		Redding	CA	96002
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. Stephanie Fultz	CICOA Aging & In-Home Solutions	8440 Woodfield Crossing Blvd	Ste 175	Indianapolis	IN	46240
10050-LE	Medicare & You 2024 (English Large Print)	10	Mrs. SONIA S VAUGHN	Ventura County Area Agency on Aging	646 County Square Dr		Ventura	CA	93003
10050-LE	Medicare & You 2024 (English Large Print)	10	Ms. Cathy A Bond	Bear River Health	2329 Center St		Boyne Falls	MI	49713
10050-LE	Medicare & You 2024 (English Large Print)	12	Emma Wilson	Social Security Administration	710 Alabama St		Bellingham	WA	98225
10050-LE	Medicare & You 2024 (English Large Print)	15	Ms. Elaine M Palmer	Social Security	901 University Dr	Ste 2	State College	PA	16801

10050-LE	Medicare & You 2024 (English Large Print)	15	Nina Yang	Milwaukee County Area Agency on Aging	1220 W Vliet St	Ste 300	Milwaukee	WI	53205
10050-LE	Medicare & You 2024 (English Large Print)	15	Pam Lovera	Fauquier County Public Library	11 Winchester St		Warrenton	VA	20186
10050-LE	Medicare & You 2024 (English Large Print)	15	Barb Templeman	Extension Library District of Huron Coun	6 W Emerald St		Willard	OH	44890
10050-LE	Medicare & You 2024 (English Large Print)	15	Michael Moldoye	Opportunity Council	1419 Cornwall Ave		Bellingham	WA	98225
10050-LE	Medicare & You 2024 (English Large Print)	20	Annette Barca	SHIBA -Whidbey Island	14594 State Route 525		Langley	WA	98260
10050-LE	Medicare & You 2024 (English Large Print)	20	Belinda Willingham SHIP/DACL	SHIP/DACL Attn Belinda Willingham	250 E St SW	6th Fl	Washington	DC	20024
10050-LE	Medicare & You 2024 (English Large Print)	20	Ann Marie Megoulas	Dauphin County Library System	4501 Ethel St		Harrisburg	PA	17109
10050-LE	Medicare & You 2024 (English Large Print)	20	Lauren Rossi	Old Bridge Public Library	1 Old Bridge Plz		Old Bridge	NJ	08857
10050-LE	Medicare & You 2024 (English Large Print)	20	Ms. Michelle Thomas	Arlington County	2100 Washington Blvd	Fl 4	Arlington	VA	22204
10050-LE	Medicare & You 2024 (English Large Print)	20	Stephanie Hood	Lifetime Resources	13091 Benedict Dr		Dillsboro	IN	47018
10050-LE	Medicare & You 2024 (English Large Print)	20	Ms. Joan Newton	Leon Mathieu Senior Center	420 Main St	2nd Fl	Pawtucket	RI	02860
10050-LE	Medicare & You 2024 (English Large Print)	20	Christinna Swearingen	Rusk County Community Library	418 Corbett Ave W		Ladysmith	WI	54848
10050-LE	Medicare & You 2024 (English Large Print)	20	Nita Ford	Lafourche Council on Aging	238 Bowie Road		Raceland	LA	70394
10050-LE	Medicare & You 2024 (English Large Print)	20	Mr. Daniel Herman	Social Security Admin	501 E Bender Blvd		Hobbs	NM	88240
10050-LE	Medicare & You 2024 (English Large Print)	20	Mr. Darryl Kalich	SSA	927 S Highway 123 Byp		Seguin	TX	78155
10050-LE	Medicare & You 2024 (English Large Print)	20	Robin Eubank-Callis	K-State Research & Extension	118 E Washington Ave		Medicine Lodge	KS	67104
10050-LE	Medicare & You 2024 (English Large Print)	20	Catherine Folk-Pushee	Johnson Public Library	275 Moore St		Hackensack	NJ	07601
10050-LE	Medicare & You 2024 (English Large Print)	20	Becky Rostron	ServiceLink Resource Center of Sullivan	180 Twistback Rd		Claremont	NH	03743
10050-LE	Medicare & You 2024 (English Large Print)	25	Mr. John Henry Crippen	Multnomah County	209 SW 4th Ave	Ste 510	Portland	OR	97204
10050-LE	Medicare & You 2024 (English Large Print)	25	Ms. Jamie Her	ADRC of Dane County	2865 N Sherman Ave		Madison	WI	53704
10050-LE	Medicare & You 2024 (English Large Print)	25	Taylor Thorn	SHIBA	1400 Queen Ave SE	Ste 102	Albany	OR	97322
10050-LE	Medicare & You 2024 (English Large Print)	25	Mr. Michael Perlman	Island Park Public Library	176 Long Beach Rd		Island Park	NY	11558
10050-LE	Medicare & You 2024 (English Large Print)	25	Rachel O'Carroll	Experience, Inc.	905 4th Ave		Warren	PA	16365
10050-LE	Medicare & You 2024 (English Large Print)	25	Ms. Charlotte E McNeely	LSCOG	2748 Wagener Rd		Aiken	SC	29801
10050-LE	Medicare & You 2024 (English Large Print)	25	Ms. Maureen M McCarthy	Strafford County ServiceLink	25 Old Dover Rd		Rochester	NH	03867
10050-LE	Medicare & You 2024 (English Large Print)	25	Cheryl Morelli	Social Security Administration	636 Pine St		Michigan City	IN	46360
10050-LE	Medicare & You 2024 (English Large Print)	25	Mrs. Yonette Backer	Social Security Administration	785 Flushing Ave	Fl 3	Brooklyn	NY	11206
10050-LE	Medicare & You 2024 (English Large Print)	25	Jenifer J Grace	etowah council on aging	623 Broad St		Gadsden	AL	35901
10050-LE	Medicare & You 2024 (English Large Print)	25	Kelly Ott	Children's Home Society of NJ	635 S Clinton Ave		Trenton	NJ	08611
10050-LE	Medicare & You 2024 (English Large Print)	25	Annie R Nersten	Upper Skagit Indian Tribe	25959 Community Plaza Way		Sedro Woolley	WA	98284
10050-LE	Medicare & You 2024 (English Large Print)	25	Beth Miller	Monmouth County Library	1001 Broad Street		Shrewsbury	NJ	07702
10050-LE	Medicare & You 2024 (English Large Print)	25	Mrs. DEBORAH FITZGERALD	AREA AGENCY ON AGING, SWA	600 Lelia		Magnolia	AR	71753
10050-LE	Medicare & You 2024 (English Large Print)	25	Ms. Phyllis Donley	Arkansas Insurance Department	1 Commerce Way		Little Rock	AR	72202
10050-LE	Medicare & You 2024 (English Large Print)	30	Ms. Pamela Gatlin	Area Agency of Aging of SWAR	600 Lelia		Magnolia	AR	71753
10050-LE	Medicare & You 2024 (English Large Print)	30	Mr. Jay Daniel Stephens	Legacy Link Inc	4080 Mundy Mill Rd		Oakwood	GA	30566

10050-LE	Medicare & You 2024 (English Large Print)	30	Mrs. Elanya Bairefoot	Palm Bay Public Library	1520 Port Malabar Blvd NE		Palm Bay	FL	32905
10050-LE	Medicare & You 2024 (English Large Print)	40	Ms. Vivian D-King	ACMS	160 N Main St	3rd Fl	Memphis	TN	38103
10050-LE	Medicare & You 2024 (English Large Print)	40	Ms. Christine R Sarracino	Pueblo of Laguna Benefits Services Progr	PO Box 194		Laguna	NM	87026
10050-LE	Medicare & You 2024 (English Large Print)	50	Sarah Nelson	City of Grand Prairie	901 Conover Dr		Grand Prairie	TX	75051
10050-LE	Medicare & You 2024 (English Large Print)	50	Mrs. Rebecca Townsend	Social Security Administration	6553 Winford Ave		Fairfield Township	OH	45011
10050-LE	Medicare & You 2024 (English Large Print)	50	Mr. David Dennewitz	Social Security Administration	550 Main St	Ste 2000	Cincinnati	OH	45202
10050-LE	Medicare & You 2024 (English Large Print)	50	Debra Rosner	Margaret E. Heggan Free Public Library	606 Delsea Dr		Sewell	NJ	08080
10050-LE	Medicare & You 2024 (English Large Print)	50	Ms. Rosalind Jones	East Central Planning and Development Di	280 Commercial Dr		Newton	MS	39345
10050-LE	Medicare & You 2024 (English Large Print)	50	Mrs. Gail S Spiewak	Chowan County Cooperative Extension	730 N Granville St	Ste A	Edenton	NC	27932
10050-LE	Medicare & You 2024 (English Large Print)	50	Mrs. Bridgette Roark-Sample	Kansas/Missouri Liscensed Health and Lif	8600 Haskell Ave		Kansas City	KS	66109
10050-LE	Medicare & You 2024 (English Large Print)	70	Amanda Marvin	BCLS	500 Center Ave		Bay City	MI	48708
10050-LE	Medicare & You 2024 (English Large Print)	100	Ms. Glenda Radical	Senior Community Services	1515 Lansdowne Ave		Darby	PA	19023
10050-LE	Medicare & You 2024 (English Large Print)	100	Frank Winter	CMS	26 Federal Plz	Fl 18	New York	NY	10278
10050-LE	Medicare & You 2024 (English Large Print)	100	Jillian McKeown	WIlmette Public Library	1242 Wilmette Ave		Wilmette	IL	60091
10050-LE	Medicare & You 2024 (English Large Print)	100	Olivia Jones	Knoxville Area Project Access	9032 Cross Park Dr		Knoxville	TN	37923
10050-LE	Medicare & You 2024 (English Large Print)	100	Erin Thompson	SSA	4 Seagate	Ste 1000	Toledo	OH	43604
10050-LE	Medicare & You 2024 (English Large Print)	100	Ardyce Mercier	SETAAAD	1000 Riverfront Pkwy		Chattanooga	TN	37402
10050-LE	Medicare & You 2024 (English Large Print)	150	Ms. Kennedy Mengerink	Social Security Administration	401 W North St	Ste 101	Lima	OH	45801
10050-LE	Medicare & You 2024 (English Large Print)	150	Lynn Bolmer	Woodbridge Public Library	1G Frederick Plaza		Woodbridge	NJ	07095
10050-LE	Medicare & You 2024 (English Large Print)	200	Mrs. Emily Dovermann	Hawaii State Library	478 S King St	Hawaii State Library - Federal Documents	Honolulu	HI	96813
10050-LE	Medicare & You 2024 (English Large Print)	200	Charlotte Hena	Pueblo of Tesuque	20 TP828		Santa Fe	NM	87506
10050-LE	Medicare & You 2024 (English Large Print)	500	Ms. KIMBERLY SIMON	SSA	5455 Bankers Ave		Baton Rouge	LA	70808
10050-LE	Medicare & You 2024 (English Large Print)	1000	Attn: PODFO	United Systems of Arkansas, Inc.	4949 West Bethany Rd		Little Rock	AR	72117
10050-LE	Medicare & You 2024 (English Large Print)	2500	Receiving Clerk	CMS	7500 Security Blvd		Baltimore	MD	21224
		7,050							

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.

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

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.

Exhibit A

CMS CLAUSE 11: CMS INFORMATION SECURITY
PAGE 1 OF 2

CMS Clause-11
CMS Information Security
Date: April 2008
Page 1 of 2

This clause applies to all organizations which possess or use Federal information, or which operate, use or have access to Federal information systems (whether automated or manual), on behalf of CMS.

The central tenet of the CMS Information Security (IS) Program is that all CMS information and information systems shall be protected from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft—whether accidental or intentional. The security safeguards to provide this protection shall be risk-based and business-driven with implementation achieved through a multi-layered security structure. All information access shall be limited based on a least-privilege approach and a need-to-know basis, i.e., authorized user access is only to information necessary in the performance of required tasks. Most of CMS' information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries, and as such, has access restrictions as required under legislative and regulatory mandates.

The CMS IS Program has a two-fold purpose:

(1) To enable CMS' business processes to function in an environment with commensurate security protections, and

(2) To meet the security requirements of federal laws, regulations, and directives.

The principal legislation for the CMS IS Program is Public Law (P.L.) 107-347, Title III, *Federal Information Security Management Act of 2002 (FISMA),* http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. FISMA places responsibility and accountability for IS at all levels within federal agencies as well as those entities acting on their behalf. _FISMA directs Office of Management and Budget (OMB) through the Department of Commerce, National Institute of Standards and Technology (NIST), to establish the standards and guidelines for federal agencies in implementing FISMA and managing cost-effective programs to protect their information and information systems. As a contractor acting on behalf of CMS, this legislation requires that **the Contractor shall**:

- Establish senior management level responsibility for IS,
- Define key IS roles and responsibilities within their organization,
- Comply with a minimum set of controls established for protecting all Federal information, and
- Act in accordance with CMS reporting rules and procedures for IS.

Additionally, the following laws, regulations and directives and any revisions or replacements of same have IS implications and are applicable to all CMS contractors.

- P.L. 93-579, *The Privacy Act of 1974,* http://www.usdoj.gov/oip/privstat.htm , (as amended);
- P.L. 99-474, *Computer Fraud & Abuse Act of 1986,* www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf P.L. 104-13,

EXHIBIT A
CMS CLAUSE 11: CMS INFORMATION SECURITY
PAGE 2 OF 2

CMS Clause-11
CMS Information Security
Date: April 2008
Page 2 of 2

Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35, www.archives.gov/federal-register/laws/paperwork-reduction;

- P.L. 104-208, *Clinger-Cohen Act of 1996* (formerly known as the Information Technology Management Reform Act), http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html;
- P.L. 104-191, *Health Insurance Portability and Accountability Act of 1996* (formerly known as the Kennedy-Kassenbaum Act) http://aspe.hhs.gov/admnsimp/pl104191.htm;
- OMB Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004, http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html;
- OMB Circular A-130, *Management of Federal Information Resources*, Transmittal 4, November 30, 2000, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html;
- NIST standards and guidance, http://csrc.nist.gov/; and,
- Department of Health and Human Services (DHHS) regulations, policies, standards and guidance http://www.hhs.gov/policies/index.html

These laws and regulations provide the structure for CMS to implement and manage a cost-effective IS program to protect its information and information systems. Therefore, **the Contractor shall** monitor and adhere to all IT policies, standards, procedures, directives, templates, and guidelines that govern the CMS IS Program, http://www.cms.hhs.gov/informationsecurity and the CMS System Lifecycle Framework, http://www.cms.hhs.gov/SystemLifecycleFramework.

The Contractor shall comply with the CMS IS Program requirements by performing, but not limited to, the following:

- Implement their own IS program that adheres to CMS IS policies, standards, procedures, and guidelines, as well as industry best practices;
- Participate and fully cooperate with CMS IS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities;
- Provide upon request results from any other audits, reviews, evaluations, tests and/or assessments that involve CMS information or information systems;
- Report and process corrective actions for all findings, regardless of the source, in accordance with CMS procedures;
- Document its compliance with CMS security requirements and maintain such documentation in the systems security profile;
- Prepare and submit in accordance with CMS procedures, an incident report to CMS of any suspected or confirmed incidents that may impact CMS information or information systems; and
- Participate in CMS IT information conferences as directed by CMS.

EXHIBIT B
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 1 OF 5

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:

EXHIBIT B
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 5 OF 5

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.

EXHIBIT C
FAQ SUPPLEMENT TO CMS SECURITY CLAUSE 09A-01
PAGE 1 OF 3

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.

Applicant Instructions for Completing Form HHS-745, "HHS ID Badge Request"

Section A collects identifying information about Applicants needed to issue an HHS ID Badge. In some Federal agencies, Sponsors or other authorized officials will complete this section for Applicants. If you are an Applicant and are asked to complete Section A, follow the instructions below. During the ID Badge issuing process, you also will be asked to complete Section F.

Clearly print all information except for your signature.

Section A

1. Check the appropriate box to indicate why a new HHS ID Badge is being issued. If you check "Other," please indicate the reason in the space provided.
2. Enter your full legal name on the first line. If you have used other name(s), enter these names on the "Other Name(s) Used" line.
3. Enter your date of birth in mm/dd/yyyy format.
4. Enter your place of birth (city and state if born in the U.S. or city and country if foreign born).
5. Enter your Social Security Number (xxx-xx-xxxx).
6. Check whether you are a U.S. citizen. If you are not a U.S. citizen, enter the country where you are a citizen.
7. Enter your position title (include series and grade level).
8. Enter where you will be working. This could include the center, office, group, division, or institute. If you are a contractor Applicant, enter the organizational chain for the COTR's or Project Officer's division.
9. Enter the physical location (building and office) of your office, work area, or contract office.
10. Enter your work telephone number. If none, then list Contract Officer's, COTR's, or Project Officer's telephone number.
11. Enter your email address.

Contractors and others employed outside the Federal government, complete items 12 through 14.

12. Enter your company's name.
13. Enter your company's address.
14. Enter your company's telephone number.

All Applicants complete items 15 and 16.

15. Sign to authorize HHS to conduct the identity proofing/verification process and to certify that you understand that actions may be taken against you if you provide false information on this form.
16. Enter the date you signed.

Sections B, C, D, and E will be completed by HHS.

Section F

You will be given a copy of the Privacy Act Statement for this HHS ID Badge Request form and HHS ID Badge Rules.

72. Sign your name to certify that you have read and understand the Privacy Act Statement and HHS ID Badge Rules and that you agree to follow the HHS ID Badge rules.
73. Enter the date of your signature.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Department of Health and Human Services (HHS) identification (ID) Badge Request

(Other Federal Departments may call this type of ID badge a Personal Identity Verifi cation [PIV] card)

HHS ID BADGE ISSUING FACILITY IDENTIFICATION NUMBER

Privacy Act Statement: The information on this form is collected by the Department of Health and Human Services (HHS) to issue you an identification badge called the HHS ID Badge. The purpose of the ID Badge is to help ensure the safety and security of government buildings, the people who work in them, and government computer systems. When you use your ID Badge an ID Badge system will verify that you are authorized to use government facilities. The system also will track and control the ID Badges that are issued. The authority to collect this information is 5 U.S.C. § 301; Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995; and Homeland Security Presidential Directive 12, August 27, 2004. The authority to request your Social Security number is Executive Order 9397. The disclosure of your Social Security number is voluntary, but it will assist in verifying your identity to process this application. The information on this form may be disclosed only with your written consent, except where permitted by the Privacy Act. The disclosures permitted by the Privacy Act include disclosure to: the Department of Justice, a court, or other government officials when the records are relevant and necessary to a law suit; the appropriate public authority (Federal, foreign, State, local, tribal, or otherwise) to enforce, investigate, or prosecute, when a record indicates a violation of law or regulation; a Member of Congress or congressional staff member at your written request; the National Archives and Records Administration for records management inspections; authorized Federal contractors, grantees, or volunteers who need access to the records to do agency work and who have agreed to comply with the Privacy Act; any source that has records an agency needs to decide whether to retain an employee, continue a security clearance, or agree to a contract, grant, license or benefi t; Federal, State, or local agencies, entities, individuals, or foreign governments to enable an intelligence agency to carry out its responsibilities; the Office of Management and Budget to evaluate private relief legislation; and to other Federal agencies to notify them when your ID Badge is no longer valid. If you do not provide all of the requested information, we may deny you an ID Badge. Without an ID Badge, you will not have access to certain Federal facilities or systems. If using an ID Badge is a condition of your employment, not providing the information may prevent you from being able to work.

A. Applicant Information *(To be completed by Applicant, Sponsor, or Authorized Official)*

1. REASON FOR ISSUANCE ☐ New Application ☐ Renewal ☐ Lost ☐ Stolen ☐ Damaged ☐ Expired
☐ Other *(specify)*: _____

2. NAME *(Last, First, Middle)* | OTHER NAME(S) USED

3. DATE OF BIRTH *(mm/dd/yyyy)* | 4. PLACE OF BIRTH City | State or Province | Country

5. SOCIAL SECURITY NUMBER *(xxx-xx-xxxx)* | 6. U.S. CITIZEN ☐ Yes ☐ No *(specify citizenship)*: _____

7. POSITION TITLE | 8. AGENCY / DIVISION

9. BUILDING / OFFICE ADDRESS | 10. WORK PHONE | 11. EMAIL

For Contractors, complete lines 12 through 14

12. ORGANIZATION / COMPANY NAME | 13. ADDRESS OF ORGANIZATION / COMPANY

14. TELEPHONE OF ORGANIZATION / COMPANY

To be completed by Applicant

I hereby authorize the release of information in this application to appropriate Federal agencies for the purposes of processing this application and verifying my identity. I also acknowledge that if I knowingly provide or assist in the provision of false information or non-verifi able information, and/or I purposely omit information, it could result in loss of access to HHS facilities and IT systems and in disciplinary action including removal from Federal service or a Federal contract, and I may be subject to prosecution under applicable Federal criminal and civil statutes.

15. APPLICANT SIGNATURE | 16. DATE *(mm/dd/yyyy)*

HHS-745 (5/07) PSC Graphics (301) 443-1090 EF **Page 1**

APPLICANT NAME

B. HHS ID Badge Request *(To be completed by Sponsor, after Section A has been completed)*

17. ID BADGE TYPE *(choose **ALL** that apply)*

☐ Foreign National ☐ HHS Employee ☐ Other Federal Employee: _____

☐ Contractor ☐ Organizational Affiliate: _____

18. EMERGENCY RESPONDER ☐ Yes ☐ No

20. ID BADGE EXPIRATION DATE *(mm/dd/yyyy)*

19. POSITION SENSITIVITY LEVEL

☐ Non-Sensitive (1) ☐ National Security/Top Secret - SCI (4)

☐ National Security/Secret or Confidential (2) ☐ Public Trust/Moderate Risk (5)

☐ National Security/Top Secret (3) ☐ Public Trust/High Risk (6)

For Contractors, complete lines 21 through 27	
PROJECT OFFICER INFORMATION *(if not Sponsor)*	
21. NAME *(Last, First, Middle)*	
22. CENTER/OFFICE/GROUP/DIVISION	
23. POSITION TITLE	
24. WORK PHONE	25. EMAIL
I certify that the above Applicant will be participating on the contract identified on this form.	
26. PROJECT OFFICER SIGNATURE	
27. DATE *(mm/dd/yyyy)*	

SPONSOR INFORMATION	
28. NAME *(Last, First, Middle)*	
29. SPONSOR ID NUMBER *(**or** complete lines 30-33)*	
30. AGENCY/DIVISION	
31. POSITION TITLE	
32. WORK PHONE	33. EMAIL
For Contractors, complete lines 34 - 36	
34. APPLICANT CONTRACT NO.	
35. CONTRACT START *(mm/dd/yyyy)*	36. CONTRACT EXPIRATION *(mm/dd/yyyy)*

I agree to sponsor the above Applicant for an HHS ID Badge and certify that the information provided in Sections A and B are complete and accurate to the best of my knowledge. I hereby acknowledge that if I knowingly provide or assist in the provision of false information, non-verifi able information, and/or I purposely omit information, I may be subject to disciplinary action up to and including removal from the Federal service and I may be subject to prosecution under applicable Federal criminal and civil statutes.

37. SPONSOR SIGNATURE	38. DATE *(mm/dd/yyyy)*

C. Identity Proofing *(To be completed by Sponsor, Enrollment Official, or Registrar after Section B has been completed)*

If the Applicant does not require a background investigation and is in possession of an undamaged, uncompromised, unexpired HHS ID Badge, you may complete all of Section C or only complete items 41-42 and 49-50.

39. COPIES OF ID SOURCE DOCUMENTS ATTACHED? ☐ Yes ☐ No

40. DID APPLICANT PRESENT TWO FORMS OF IDENTIFICATION, ONE OF WHICH WAS A PHOTO ID ISSUED BY A STATE OR THE FEDERAL GOVERNMENT? ☐ Yes ☐ No

IDENTITY PROOFER INFORMATION
41. NAME (LAST, FIRST, MIDDLE)
42. IDENTITY PROOFER ID NUMBER

IDENTITY SOURCE DOCUMENT ONE
43. NAME
44. DOC. TITLE
45. DOC. EXPIRATION DATE *(mm/dd/yyyy)*

IDENTITY SOURCE DOCUMENT TWO
46. NAME
47. DOC. TITLE
48. DOC. EXPIRATION DATE *(mm/dd/yyyy)*

I certify that the above Applicant appeared before me and presented two ID source documents, which to the best of my knowledge appeared to be genuine, or presented an undamaged uncompromised, unexpired HHS ID Badge and does not require a background investigation. I hereby acknowledge that if I knowingly provide or assist in the provision of false information, non- verifiable information, and/or I purposely omit information, I may be subject to disciplinary action up to and including removal from the Federal service, and I may be subject to prosecution under applicable Federal criminal and civil statutes.

49. ID PROOFER SIGNATURE	50. DATE *(mm/dd/yyyy)*

APPLICANT NAME

D. HHS ID Badge Approval *(To be completed by Registrar, after Section C has been completed)*

If the Applicant does not require a background investigation and is in possession of an undamaged, uncompromised, unexpired HHS ID Badge, you may complete all of Section D or only complete items 51 and 57-60.

51. RECIPROCITY VERIFIED *(if applicable)*
PIPS RECORD ATTACHED
☐ Yes ☐ No ☐ Not applicable

52. TYPE OF BACKGROUND INVESTIGATION TO COMPLETE
☐ SAC ☐ CNACI ☐ ANACI ☐ BI
☐ NAC ☐ NACIC ☐ MBI ☐ SSBI
☐ NACI ☐ NACLC ☐ LBI ☐ SSBI-PR

53. FBI FINGERPRINT CHECK RESULTS RECEIVED *(mm/dd/yyyy)*

54. FAVORABLE RESULTS? ☐ Yes ☐ No

55. BACKGROUND INVESTIGATION COMPLETED *(mm/dd/yyyy)*

56. COMMENTS

REGISTRAR INFORMATION
57. NAME *(Last, First, Middle)*
58. REGISTRAR ID NUMBER

I hereby ☐ Approve ☐ Disapprove issuance of an HHS ID Badge to the above-named Applicant. I hereby acknowledge that if I knowingly provide or assist in the provision of false information, non-verifiable information, and/or I purposely omit information, I may be subject to disciplinary action up to and including removal from the Federal service, and I may be subject to prosecution under applicable Federal criminal and civil statutes.

59. REGISTRAR SIGNATURE

60. DATE *(mm/dd/yyyy)*

E. HHS ID Badge Details *(To be completed by Issuer, after Section D has been completed)*

61. NAME ON ID BADGE

62. ID BADGE NUMBER

63. ID BADGE EXPIRATION DATE *(mm/dd/yyyy)*

ISSUER INFORMATION
64. NAME *(Last, First, Middle)*
65. ISSUER ID NUMBER

☐ I confirm that the (1) ID Badge Request received from the Sponsor is valid, and (2) approval notification received from the Registrar is valid.

☐ I have verified that the individual collecting the ID Badge is the Applicant and have issued the ID Badge to the Applicant.

☐ I have mailed the ID Badge and this form to _____

in Remote Office _____ on this date (mm/dd/yyyy) _____.

I hereby acknowledge that if I knowingly provide or assist in the provision of false information, non-verifiable information, and/ or I purposely omit information, I may be subject to disciplinary action up to and including removal from the Federal service, and I may be subject to prosecution under applicable Federal criminal and civil statutes.

66. ISSUER SIGNATURE

67. DATE *(mm/dd/yyyy)*

FOR REMOTE ISSUERS ☐ I have verified that the individual collecting the ID Badge is the Applicant and have issued the ID Badge to the Applicant.

68. REMOTE ISSUER NAME *(Last, First, Middle)*

69. REMOTE ISSUER ID

70. REMOTE ISSUER SIGNATURE

71. DATE *(mm/dd/yyyy)*

F. Applicant Acknowledgement *(To be completed by Applicant, after Section E has been completed)*

I have read and understand the Privacy Act Statement and HHS ID Badge Rules that were given to me. I accept the HHS ID Badge and agree to abide by the HHS ID Badge Rules.

72. APPLICANT SIGNATURE

73. DATE *(mm/dd/yyyy)*

Privacy Act Statement *(Applicant Copy)*

The information on this form is collected by the Department of Health and Human Services (HHS) to issue you an identification badge called the HHS ID Badge. The purpose of the ID Badge is to help ensure the safety and security of government buildings, the people who work in them, and government computer systems. When you use your ID Badge an ID Badge system will verify that you are authorized to use government facilities. The system also will track and control the ID Badges that are issued. The authority to collect this information is 5 U.S.C. § 301; Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995; and Homeland Security Presidential Directive 12, August 27, 2004. The authority to request your Social Security number is Executive Order 9397. The disclosure of your Social Security number is voluntary, but it will assist in verifying your identity to process this application.

The information on this form may be disclosed only with your written consent, except where permitted by the Privacy Act. The disclosures permitted by the Privacy Act include disclosure to: the Department of Justice, a court, or other government officials when the records are relevant and necessary to a law suit; the appropriate public authority (Federal, foreign, State, local, tribal, or otherwise) to enforce, investigate, or prosecute, when a record indicates a violation of law or regulation; a Member of Congress or congressional staff member at your written request; the National Archives and Records Administration for records management inspections; authorized Federal contractors, grantees, or volunteers who need access to the records to do agency work and who have agreed to comply with the Privacy Act; any source that has records an agency needs to decide whether to retain an employee, continue a security clearance, or agree to a contract, grant, license or benefi t; Federal, State, or local agencies, entities, individuals, or foreign governments to enable an intelligence agency to carry out its responsibilities; the Office of Management and Budget to evaluate private relief legislation; and to other Federal agencies to notify them when your ID Badge is no longer valid.

If you do not provide all of the requested information, we may deny you an ID Badge. Without an ID Badge, you will not have access to certain Federal facilities or systems. If using an ID Badge is a condition of your employment, not providing the information may prevent you from being able to work.

Department of Health and Human services (HHS) ID Badge Rules *(Applicant Copy)*

The rules associated with the HHS ID Badge include but are not limited to

- Do not attempt to clone, modify, or obtain data from any HHS ID Badge.
- Protect and safeguard your ID Badge.
- If your ID Badge is lost or stolen, you must report the missing ID Badge within 24 hours of noting its disappearance. Your ID Badge will be disabled and you will have to apply for a replacement.
- If you become aware of any violation of these requirements or suspect that your ID Badge may have been used by someone else, immediately report that information to your agency's ID Badge issuing authority.
- You must request a new ID Badge within 30 days in the event of any change which may affect the ability to determine that you are the individual associated with the ID Badge (e.g., name change). You will provide documentation showing the reason for any such change where applicable.
- As part of the HHS exit process, you are to return your ID Badge to the designated official at your agency on your last day of employment at HHS or at the expiration of your authorized access to HHS facilities and/or IT systems.
- Do not attempt to assist others in gaining unauthorized access to Federal facilities or information. Accept responsibility for the whereabouts and conduct of any and all persons whom you have signed in (i.e., authorized admittance) to HHS facilities. All persons signed into HHS facilities are considered visitors. Only visitor badges will be issued.
- Do not disclose or lend your identification number and/or password to someone else to gain access to HHS IT systems. 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 access or illegal transactions.

EXHIBIT E
APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS (FORM CMS-20037)
PAGE 1 OF 3

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

EXHIBIT E
APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS (FORM CMS-20037)
PAGE 2 OF 3

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.

Form CMS-20037 (09/05) EF 09/2005 Page 2

EXHIBIT E
APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS (FORM CMS-20037)
PAGE 3 OF 3

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

Form CMS-20037 (09/05) EF 09/2005 Page 3

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.

EXHIBIT F
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 2 OF 6

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

CMS Contract No. *(If applicable)*
Program 1583-S

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).

Form CMS-R-0235 (05/08) 2

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

File	Years(s)	System of Record

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* 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	

EXHIBIT F
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 6 OF 6

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 G
CERTIFICATE OF DATA DESTRUCTION (FORM CMS-10252)
PAGE 1 OF 2

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

Form Approved
OMB No. 0938-1046

INSTRUCTIONS FOR COMPLETING THE CERTIFICATE OF DATA DESTRUCTION FOR DATA ACQUIRED FROM THE CENTERS FOR MEDICARE & MEDICAID SERVICES

This certificate is to be completed and submitted to CMS to certify the destruction of all CMS data covered by the listed Data Use Agreement (DUA). This includes any copies made of the files, any derivative or subsets of the files, and any manipulated files. The requestor may not keep any copies, derivative or manipulated files—all files must be destroyed. CMS will close the listed DUA upon receipt and review of this certificate.

Directions for the completion of the certificate follow:

- Complete the Requestor and Custodian's Organization and Contact information as listed in the DUA.
- Provide the DUA number.
- Provide the Project/Study Name as listed on the DUA.
- Provide the CMS Project Officer, if applicable.
- Please list all data files and years covered by the DUA.
- A signature is required on this certification. The signature should be the requestor or Custodian listed on the DUA. If the DUA is for a CMS Contract/Demonstration, the CMS Project Officer must also sign the certificate.

Please submit this certificate to:

Director, Division of Privacy Compliance
Division of Privacy Compliance
Mailstop: N2-04-27
7500 Security Blvd.
Baltimore, MD 21244

EXHIBIT G
CERTIFICATE OF DATA DESTRUCTION (FORM CMS-10252)
PAGE 2 OF 2

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CERTIFICATE OF DATA DESTRUCTION FOR DATA ACQUIRED FROM THE CENTERS FOR MEDICARE & MEDICAID SERVICES

REQUESTOR ORGANIZATION	DATA USE AGREEMENT (DUA) NO.
REQUESTOR CONTACT NAME	PHONE NO.
REQUESTOR ADDRESS	
CUSTODIAN ORGANIZATION	
CUSTODIAN CONTACT NAME	
CUSTODIAN ADDRESS	PHONE NO.
PROJECT/STUDY NAME	
CMS PROJECT OFFICER *(IF APPLICABLE)*	

CMS Data Files Destroyed:	**Files**	**Years**

By signing this Certification of Data Destruction, I confirm that the data acquired under DUA # _____ have been completely destroyed and no copies have been kept.

REQUESTOR OR CUSTODIAN PRINTED NAME	SIGNATURE	DATE
CMS PROJECT OFFICER *(IF APPLICABLE)* PRINTED NAME	SIGNATURE	DATE

Form CMS-10252 (12/07) 2

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.

-3-

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.

-4-

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.