Program No 55-S Term Date of Award To 05/31/13
TITLE: "Medicare and You Mailing List Services"

			L&D MAIL MASTERS New Albany, IN		MIDWEST DIRECT Cleveland, OH		PEACHTREE DATA Duluth, GA	
		Basis of AWARD	Unit Rate	Cost	Unit Rate	Cost	Unit Rate	Cost
I.	MAIL FILE PROCESSING:							
a.	**CASS/NCOA Processing…….**							
	per 1000 records input……..							
1	up to 20,000 Records……	20	$ 2.20	$ 44.00	$ 3.00	$ 60.00	$ 0.25	$ 5.00
2	500,000 to 10,000,000 Records	1000	$ 2.20	$ 2,200.00	$ 0.65	$ 650.00	$ 0.15	$ 150.00
3	10,000,001 to 41,000,000 Records	41000	$ 2.20	$ 90,200.00	$ 0.45	$ 18,450.00	$ 0.15	$ 6,150.00
b.	**Deceased Coding..per 1000**							
	records input……..							
1	up to 20,000 Records……	20	$ 1.27	$ 25.40	$ 1.49	$ 29.80	N/C	$ -
2	500,000 to 10,000,000 Records	1000	$ 1.27	$ 1,270.00	$ 1.49	$ 1,490.00	N/C	$ -
3	10,000,001 to 41,000,000 Records	41000	$ 1.27	$ 52,070.00	$ 1.43	$ 58,630.00	N/C	$ -
c.	**Deceased Coding ..per 1000**							
	records matched……..							
1	up to 20,000 Records……	0.2	N/C	$ -	N/C	$ -	$ 35.00	$ 7.00
2	500,000 to 10,000,000 Records	100	N/C	$ -	N/C	$ -	$ 35.00	$ 3,500.00
3	10,000,001 to 41,000,000 Records	410	N/C	$ -	N/C	$ -	$ 35.00	$ 14,350.00
d.	**Apartment Append…per 1000**							
	record input……							
1	up to 20,000 Records……	20	$ 13.80	$ 276.00	$ 1.00	$ 20.00	N/C	$ -
2	500,000 to 10,000,000 Records	1000	$ 13.80	$ 13,800.00	$ 0.60	$ 600.00	N/C	$ -
3	10,000,001 to 41,000,000 Records	41000	$ 13.80	$ 565,800.00	$ 0.38	$ 15,580.00	N/C	$ -
e.	**Apartment Append…per 1000**							
	matched……..							
1	up to 20,000 Records……	0.5	N/C	$ -	N/C	$ -	$ 8.00	$ 4.00
2	500,000 to 10,000,000 Records	250	N/C	$ -	N/C	$ -	$ 8.00	$ 2,000.00
3	10,000,001 to 41,000,000 Records	1025	N/C	$ -	N/C	$ -	$ 8.00	$ 8,200.00
f.	**De-Duping..per 1000 records input..**							
1	up to 20,000 Records……	20	$ 5.75	$ 115.00	$ 3.00	$ 60.00	$ 1.00	$ 20.00
2	500,000 to 10,000,000 Records	1000	$ 5.75	$ 5,750.00	$ 3.00	$ 3,000.00	$ 0.25	$ 250.00
3	10,000,001 to 41,000,000 Records	41000	$ 5.75	$ 235,750.00	$ 0.99	$ 40,590.00	$ 0.20	$ 8,200.00
II.	ADDITIONAL ..OPERATIONS:							
a.	**System Time Work…per hour…**	20	$ 85.00	$ 1,700.00	$ 85.00	$ 1,700.00	N/C	$ -
	CONTRACTOR TOTALS			$ 969,000.40		$ 140,859.80		$ 42,836.00
	DISCOUNT		0.0%	$ -	20.0%	$ 28,171.96	0.0%	$ -
	DISCOUNTED TOTALS			$ 969,000.40		$ 112,687.84		$ 42,836.00

AWARDED

U.S. GOVERNMENT PRINTING OFFICE

Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

"Medicare and You Mailing List Services"

as requisitioned from the U.S. Government Printing Office (GPO) by the

Department of Health and Human Services/Centers for Medicare and Medicaid Services

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning Date of Award and ending May 31, 2013 plus up to four optional 12-month extension period(s) that may be added in accordance with the "Option to Extend the Term of the Contract" clause in Section 1 of this contract.

BID OPENING: Bids shall be publicly opened at 11 a.m., prevailing Washington, DC time, on June 4, 2012.

BID SUBMISSION: Submit bid in pre-addressed envelope furnished with solicitation, or send to: U.S. Government Printing Office, Bid Section, 36H Street NW, Room C–161, Washington, DC 20401. Facsimile bids in response to this solicitation are permitted. Facsimile bids may be submitted directly to the GPO Bid Section, FAX No. (202) 512-1782. The Program Number and bid opening date must be specified with the bid. Refer to Facsimile Bids in Solicitation Provisions of GPO Contract Terms, GPO Publication 310.2 as revised June 2001.

THIS IS A NEW PROGRAM. THERE IS NO ABSTRACT AVAILABLE.

For information of a technical nature call Marty Janney on (202) 512-1164 (No collect calls) or email tjanney@gpo.gov.

SECTION 1. – GENERAL TERMS AND CONDITIONS

GPO CONTRACT TERMS: Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Pub. 310.2, Rev. June 2001) and GPO Contract Terms, Quality Assurance Through Attributes Program (GPO Pub. 310.1, effective April 1996, Rev. August 2002).

GPO Publication 310.2, GPO Contract Terms, Contract Clause 5. Disputes, is hereby replaced with the June 2008 clause found at www.gpo.gov/pdfs/vendors/contractdisputes.pdf. This June 2008 clause also cancels and supersedes any other disputes language currently included in existing contractual actions.

EXTENSION OF CONTRACT TERM: At the request of the Government, the term of any contract resulting from this solicitation may be extended for such period of time as may be mutually agreeable to the GPO and the contractor.

OPTION TO EXTEND THE TERM OF THE CONTRACT: The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed five years as a result of, and including, any extension(s) added under this clause. Further extension may be negotiated under the "Extension of Contract Term" clause. See also "Economic Price Adjustment" for authorized pricing adjustment(s).

ECONOMIC PRICE ADJUSTMENT: The pricing under this contract shall be adjusted in accordance with this clause, provided that in no event will any pricing adjustment be made that would exceed the maximum permissible under any law in effect at the time of the adjustment. There will be no adjustment for orders placed during the first period specified below. Pricing will thereafter be eligible for adjustment during the second and any succeeding performance period(s). For each performance period after the first, a percentage figure will be calculated as described below and that figure will be the economic price adjustment for that entire next period. Pricing adjustments under this clause are not applicable to reimbursable postage or transportation costs, or to paper, if paper prices are subject to adjustment by separate clause elsewhere in this contract.

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from the beginning of the contract to May 31, 2013 and the second and any succeeding period(s) will extend for 12 months from the end of the last preceding period, except that the length of the final period may vary. The first day of the second and any succeeding period(s) will be the effective date of the economic price adjustment for that period.

Pricing adjustments in accordance with this clause will be based on changes in the seasonally adjusted "Consumer Price Index For All Urban Consumers - Commodities Less Food" (Index) published monthly in the CPI Detailed Report by the U.S. Department of Labor, Bureau of Labor Statistics.

The economic price adjustment will be the percentage difference between Index averages as specified in this paragraph. An index called the variable index will be calculated by averaging the monthly Indexes from the 12-month interval ending 3 months prior to the beginning of the period being considered for adjustment. This average is then compared to the average of the monthly Indexes for the 12-month interval ending February 29, 2012, called the base index. The percentage change (plus or minus) of the variable index from the base index will be the economic price adjustment for the period being considered for adjustment.

The Government will notify the contractor by contract modification specifying the percentage increase or decrease to be applied to invoices for orders placed during the period indicated. The contractor shall apply the percentage increase or decrease against the total price of the invoice less reimbursable postage or transportation costs and separately adjusted paper prices. Payment discounts shall be applied after the invoice price is adjusted.

ASSIGNMENT OF JACKETS, PURCHASE AND PRINT ORDERS: A GPO jacket number will be assigned and a purchase order issued to the contractor to cover work performed. The purchase order will be supplemented by an individual "Print Order" for each job placed with the contractor. The print order, when issued, will indicate the quantity to be produced and any other information pertinent to the particular order.

POST AWARD CONFERENCE: The total requirements of the job as indicated in these specifications will be reviewed by Government representatives with the contractor's representatives at the GPO, Washington, DC immediately after award.

ORDERING: Items to be furnished under the contract shall be ordered by the issuance of print orders by the Government. Orders may be issued under the contract from date of award through May 31, 2013, plus for such additional period(s) as the contract is extended. All print orders issued hereunder are subject to the terms and conditions of the contract. The contract shall control in the event of conflict with any print order. A print order shall be "issued" for purposes of the contract, when it is either deposited in the U.S. Postal Service mail or otherwise furnished to the contractor in conformance with the schedule.

REQUIREMENTS: This is a requirements contract for the items and for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "Ordering." The quantities of items specified herein are estimates only, and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated," it shall not constitute the basis for an equitable price adjustment under this contract.

Except as otherwise provided in this contract, the Government shall order from the contractor all the items set forth which are required to be purchased by the Government activity identified on page 1.

The Government shall not be required to purchase from the contractor, requirements in excess of the limit on total orders under this contract, if any.

Orders issued during the effective period of this contract and not completed within that time shall be completed by the contractor within the time specified in the order, and the rights and obligations of the contractor and the Government respecting those orders shall be governed by the terms of this contract to the same extent as if completed during the effective period of this contract.

If shipment/delivery of any quantity of an item covered by the contract is required by reason of urgency prior to the earliest date that shipment/delivery may be specified under this contract, and if the contractor will not accept an order providing for the accelerated shipment/delivery, the Government may procure this requirement from another source.

The Government may issue orders which provide for shipment/delivery to or performance at multiple destinations.

Subject to any limitations elsewhere in this contract, the contractor shall furnish to the Government all items set forth herein which are called for by print orders issued in accordance with the "Ordering" clause of this contract.

SECTION 2. – SPECIFICATIONS

SCOPE: To sanitize mail list files of recipients receiving Medicare and You Handbooks, in order to enhance the accuracy of addresses and reduce the number of multiple handbooks that are delivered to a household with multiple beneficiaries.

TITLE: "Medicare and You Mailing List Services"

FREQUENCY OF ORDERS: 1 to 2 Test Orders and 3 to 4 Live Orders per year.

QUANTITY PER ORDER: Up to 20,000 records per Test Order; 500,000 to 41,000,000 records per Live Order.

Phase One and Phase Two: CMS may provide the contractor with three test mailing address files. These three files will contain approximately 29 mailing addresses, 783 mailing addresses, and 14,634 mailing addresses and will be sent to contractor via an electronic Gentran mailbox. These files contain names and addresses (record sheet layout attached). Test files will be used to verify contractor is counting the number of mail files correctly during the duplicate removal process.

Phase One: Initial Test Files

Step 1: The contractor will run these three files through Coding Accuracy Support System (CASS), National Change of Address (NCOA), Deceased Coding, and Apartment Append Coding. The NCOA must include 48-month licensing, CASS, DPV, LACS Link, and Suite Link.

Step 2: The contractor will remove all undeliverable and deceased addresses per CASS/NCOA/Deceased Coding from each mailing address file. Undeliverable addresses should be counted for each file and added to the Report Summary spreadsheet (format in table 2 below). The contractor will then create an Excel file of these addresses called "file abc cleaned" in the format as outlined in Table 1:

Table 1:
Name/address Excel files are formatted with separate columns for:
rep payee (if applicable)
last name
first name
middle initial
address line 1
address line 2
etc.

Step 3: The contractor will deliver to CMS one Excel spreadsheet for each mail file. These will be delivered by email and the files will be password protected. The spreadsheets will contain all the addresses from the mail file with just the CASS/NCOA updates and the undeliverable addresses removed (detailed in step 2).

Phase Two: Revised Test Files (after Phase One)

Step 1: The contractor will then remove duplicate addresses and count the addresses on each file in the following manner:

a. Any address that appears only 1 time is counted as one address.
b. Any address that appears 2, 3, or 4 times will have all but one of that address removed and that address is then counted as one address. All duplicates should be removed at the address level. Any address appearing more than one time in this category should be deleted regardless of the household name.
c. Any address that appears 5 times or more will all be counted as unique addresses, and none of these addresses will be removed.

Example One: "123 Maple Street, Woodlawn, MD 21224" appears 3 times. Therefore, 2 of these addresses will be removed. This address will be counted as 1 address.
Example Two: "123 Maple Street, Woodlawn, MD 21224" appears 3 times. . The addresses appear under the names Bob Smith, Martha Smith and John Jones. Therefore, 2 of these addresses will be removed. This address will be counted as 1 address.
Example Three: "456 Oak Street, Washington, DC 28045" appears 6 times. None of these addresses will be removed. This address will be counted as 6 addresses.

Step 2: The contractor will deliver to CMS one Excel spreadsheet for each mail file. These will be delivered by email and the files will be password protected. The spreadsheets will contain all the addresses with the clean-up of duplicates removed (detailed in step 1).

CMS will evaluate contractor results and discuss any concerns with the contractor.

For each address file there should be a report summary of the total number of addresses, after Step 1 has been completed. The report summary should match up with the total number of addresses in your net file after clean up of duplicates.

Table 2:
Report Summary example:

Mail file names	# of addresses that appear only once	# of addresses that appear 2 to 4 times	# of addresses that appear 5 or more times	# of undeliverable addresses per CASS/NCOA
Mail file abc	25,000	48,000	6,000	
Mail file xyz	20,000	40,000	3,000	
.....	.....	.....	.....	
Totals				

Phase Three - Live Files:
Step 1: CMS will provide approximately 60 live electronic files containing approximately 41,000,000 mailing addresses to the contractor via an electronic Gentran mailbox. The files contain a total of approximately 41,000,000 records containing names and addresses (record sheet layout attached). Contractor will run these files through Coding Accuracy Support System (CASS), National Change of Address (NCOA), Deceased Coding, Apartment Append Coding, and De-Duping The NCOP must include 48-month licensing, CASS, DPV, LACS Link, and Suite Link.

Step 2: The contractor will remove all undeliverable and deceased addresses per CASS/NCOA/Deceased Coding from each mailing address file.

Undeliverable addresses should be counted for each file and added to the Report Summary spreadsheet required in step 4.

Step 3: The contractor will then remove duplicate addresses and count the addresses on each file in the following manner:

a. Any address that appears only 1 time is counted as one address.
b. Any address that appears 2, 3, or 4 times will have all but one of that address removed and that address is then counted as one address. **All duplicates should be removed at the address level.** Any address appearing more than one time in this category should be deleted regardless of the household name.
c. Any address that appears 5 times or more will all be counted as unique addresses, and **none** of these addresses will be removed.

Example One: "123 Maple Street, Woodlawn, MD 21224" appears 3 times. Therefore, 2 of these addresses will be removed. This address will be counted as 1 address.
Example Two: "123 Maple Street, Woodlawn, MD 21224" appears 3 times. . The addresses appear under the names Bob Smith, Martha Smith and John Jones. Therefore, 2 of these addresses will be removed. This address will be counted as 1 address.
Example Three: "456 Oak Street, Washington, DC 28045" appears 6 times. None of these addresses will be removed. This address will be counted as 6 addresses.

Step 4: Contractor will provide CMS with an Excel spreadsheet Report Summary (formatted like table 2 above) for all of the live files.

Contractor will also provide CMS with an Excel spreadsheet containing all live file names and the final number of addresses per file. This summary will be the total number of mailing addresses per file to which a copy of the Medicare & You book will be sent. See Table 3 for format.

Table 3:
Final Address tally:

Mail file name	# of addresses
Mail file abc	1,482,000
Mail file xyz	290,000
.....	.....
Totals	

Step 5: CMS will evaluate contractor results and discuss any concerns with the contractor. Once CMS has given approval, contractor will then provide to CMS approximately 60 cleaned-up files with duplicates removed. The contractor will save these files back into the Gentran mailbox. (Instructions to follow)

Note: These final address files should follow the same record layout as provided. Names or parts of the address should not shift in the layout.

Phase Four – Identification and Removal of addresses appearing more than 30 times:

The contractor must identify any address that appears more than 30 times in a mail file and CMS must have the option of removing some of those addresses from a mail file. For example, if an address appears 35 times on a mail file CMS may instruct the contractor to delete all but 5 of those addresses. For addresses appearing more than 30 times in a mail file, the contractor is to provide an Excel spreadsheet listing each address and how many times it appeared.

PROJECT PLAN:

Preaward Surveys: The Government will conduct a review of all data handling involved along with their specific functions, and the contractor's/subcontractor's, personnel, production, security and other requirements outlined in this contract and in the contractor's Security Plan.

The Contractor must present a detailed Project Plan **prior to award** and five (5) business days after notification by Marty Janney, which will include the following:

Security of Personally Identifiable Information (PII) is a vital component of this contract.
The Contractor shall guarantee strict confidentiality, integrity, and limited availability of all PII provided by the Government during the performance of this contract. Disclosure of the information/data, in whole or in part, by the Contractor can only be made in accordance with the provisions in the Data Use Agreement (DUA). See Security Exhibit 6.

It is the contractor's responsibility to properly safeguard PII from loss, theft, or inadvertent disclosure and to immediately notify the Government of any loss of personally identifiable information. PII for the Medicare & You handbook includes: a person's name and address.

The contractor shall not release, or sell, to any person any technical or other data received from the Government under the contract; nor shall the contractor use the data for any purpose other than that for which it was provided to the contractor under the terms of the contract. The contractor must guarantee that furnished PII will be used only to complete this contract.

Proper control and handling must be maintained at all times to prevent any information or materials required to produce the products ordered under these specifications from falling into unauthorized hands. All PII furnished by the Government, or duplicates created by the contractor or their representatives, and any resultant printouts must be kept accountable and under security to prevent their release to unauthorized persons. Unsecured telecommunications, including the internet, to transmit PII is prohibited.

Data Custodians: If any PII is to be forwarded to additional contractor-owned locations or to sub- contractor-owned locations, all security requirements also apply to those locations (all parties involved). The contractor is responsible for the actions of all locations. The contractor's project manager shall appoint up to two Data Custodians at each location and shall have them complete an Addendum to Data Use Agreement. See Security Exhibit 7: Addendum to Data Use Agreement (DUA). The contractor's project manager must collect and submit completed forms to CMS before any PII may be sent to that location.

Personnel Security: The contractor shall have a system in place to perform criminal background investigations and Social Security Number verification on all employees. In addition, CMS will perform background investigations on two contractor employees who will access the Gentran mailbox. See Security Exhibits 2, 3, 4, and 5 for more information.

Physical Security: The contractor shall have a secure work area(s) for processing and production of all CMS PII in electronic and paper format. The work area(s) shall be accessible only to authorized employees, and all work shall be monitored closely by contractor management, while CMS PII is being processed and/or produced.

Information Technology (IT) Security: The contractor shall have a system in place to comply with CMS Information Security Clause 11 in Security Exhibit 1.

Security Liaison(s): The contractor must appoint one or more Security Liaison(s) to handle issues regarding personnel, physical, and computer security; confidential issues that may arise at any point during the background investigation process; and to serve as a point of contract to the Government for security issues. The Liaison's duties will include attending the Postaward Conference, submitting a security plan, discussing confidential security issues with CMS staff, submitting background applications, and resolving any issues of inaccurate or incomplete data supplied by background investigation applicants. In the event CMS discovers sensitive information during the background investigation, CMS Security may need to contact the background investigation applicant directly.

Disposal of Waste Material: All waste material containing PII must be destroyed in a manner that it is not possible to recreate the product or identity of a beneficiary; i.e. burning, pulping, shredding, macerating, or other suitable means. If the contractor selects shredding as a means of destruction, it must be a cross cut shredder with a maximum size of 5/32" x 1-1/2" cross cut particles. Strip shredding is not acceptable. Destruction of waste must occur inside the contractor's secure production facility, close to the point of production or inspection. Sending intact waste containing PII to a municipal incinerator, or to a recycler, or any other off-site processor, is not acceptable and will be considered a data breach.

Disposal of Electronic PII: Immediately after production of each print order is complete, all electronic files containing PII furnished for the print order must be permanently destroyed in accordance with Federal Information Security Management Act (FISMA) of 2002. CMS will maintain an archive of furnished files.

Incident Reporting Requirements: If there is a breach, or a suspected breach, of Personally Identifiable Information (PII), the incident must be reported to CMS within one hour of discovery. Report breaches to the CMS IT Service Desk at 410-786-2580 or 800-562-1963.

Expiration of Data Use Agreement (DUA): Upon expiration of this DUA, the contractor will be required to sign a certificate confirming destruction of all CMS data files and that no copies have been kept. Failure to certify file destruction may cause the CMS Privacy Office to refuse to issue future DUA's and data with the contractor's company or to individuals listed on this DUA. See Exhibit 8: Certificate of Data Destruction. The contractor representative named in Section 16 of the DUA may sign one certificate for all locations.

Security Exhibits: The following exhibits 1 through 9 (see attached, 33 total pages) contain security clauses, information, and forms.

- Security Exhibit 1: CMS Clause 11: CMS Information Security (April 2008)
- Security Exhibit 2: CMS Clause 09A-01 Security Clause (May 2007)
- Security Exhibit 3: FAQ Supplement to CMS Security Clause 09A-01 (April 2008)
- Security Exhibit 4: HHS Identification ID) Badge Request (Form HHS-745) (05/07))
  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. This form is to be submitted to CMS immediately after award and renew annually thereafter.
- Security Exhibit 5: Application for Access to CMS Computer Systems (This form no longer needs to be filled out. Applicants will need to go online to apply for access to the Gentran mailbox.)
- Security Exhibit 6: Data Use Agreement (DUA) (Form CMS-R-0235 (06/10))
  Contractor management must complete CMS-R-0235, and submit to CMS immediately after award.
- Security Exhibit 7: Addendum to Data Use Agreement (DUA) (Form CMS-R-0235A (03/06)) Data Custodians at each location must complete CMS-R-0235A. Contractor's project manager must collect and submit completed forms to CMS before any PII may be sent to that location.
- Security Exhibit 8: Certificate of Data Destruction (Form CMS-10252 (12/07))
  Contractor must complete CMS-10252 at the expiration of the DUA.
- Security Exhibit 9: Secure One HHS, Information Security Program Rules of Behavior (2/12/08)) All contractor management and employees involved in this contract must read and sign this document. Signed copies of this document for Gentran applicants, DUA applicants, and Data Custodians must be submitted to CMS immediately after 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) to: CMS, Attn: Pat McNaughton, SL-11-16, 7500 Security Blvd, Baltimore, MD 21244. For delivery directly to Pat McNaughton, the contractor should use FedEx Overnight service and use FedEx furnished packaging. All other delivery services and packaging are opened and inspected in the CMS mailroom.

Security Plan: The contractor must have a formal, documented Security Plan that will ensure their compliance with all of the security provisions of this contract and as referenced in attached exhibits. Particular attention should be given to addressing compliance of the *Federal Information Security Management Act of 2002 (FISMA)* and the *Privacy Act of 1974* as referenced in Exhibit 1, CMS Clause 11.

Minimum security requirements for FISMA compliance are defined by the Department of Commerce, National Institute of Standards and Technology (NIST) in Federal Information Processing Standards Publication (FIPS) Publication 200 "Minimum Security Requirements for Federal Information and Information Systems". This document can be found on the internet at: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf .

Contractor must submit their Security Plan with their Project Plan. Release of PII by CMS does not constitute CMS' approval or acceptance of the Security Plan. At any time during this contract, if CMS finds deficiencies in the Security Plan, CMS may require correction of the deficiency.

GOVERNMENT TO FURNISH:

Mailing addresses, via an electronic Gentran mailbox.

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

A copy of the Government furnished certificate must accompany the invoice sent to GPO, Financial Management Service, for payment. Failure to furnish the certificate may result in delay in processing the invoice.

A copy of e-mail from HHS/CMS confirming receipt of acceptable mail files and identified by Program, Jacket and Print Order numbers, must be furnished with billing as evidence of delivery.

DISTRIBUTION: Deliver completed mail lists to CMS' secure Gentran mailbox.

SCHEDULE:

Adherence to each part of this schedule must be maintained. Contractor must not start production of any job prior to receipt of the individual print order (GPO Form 2511).

The ship/deliver date indicated on the print order is the date products ordered must be delivered to the destination(s) specified.

The following schedule begins the workday after notification of the availability of print order and furnished files; the workday after notification will be the first workday of the schedule.

Delivery of **Phase One** deliverable (Excel spreadsheet) must be made within two (2) workdays after receipt of print order and furnished files.

Delivery of **Phase Two** deliverable (Excel spreadsheet) must be made within two (2) workdays after agency approval to move forward after Phase One.

Delivery of **Phase Three, Step 4 and Phase Four** deliverables (Excel spreadsheets) must be made within seven (7) workdays after receipt of print order and furnished files.

Delivery of **Phase Three, Step 5** completed sanitized mail file list (with customer requested corrections), deliverable (Excel spreadsheet) must be made within three (3) workdays after notification of requested corrections.

Upon completion of each order, the contractor is to notify the U.S. Government Printing Office of the date of shipment (or delivery, if applicable). Call (202) 512-0516 or (202) 512-0517: callers outside the Washington, DC area may call toll free 1-800-424-9470 or 1-800-424-9471.

SECTION 3. – DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices offered in the "Schedule of Prices" to the following units of production which are the estimated requirements to produce one year's production under this contract. These units do not constitute, nor are they to be construed as, a guarantee of the volume of work which may be ordered under this contract for a like period of time.

The following item designations correspond to those listed in the "Schedule of Prices".

		(1)	(2)	(3)
I.	(a)	20	1000	41000
	(b)	20	1000	41000
	(c)	18	990	39600
	(d)	20	1000	41000
	(e)	2	4	8
	(f)	20	1000	41000

II.	(a)	20

SECTION 4. – SCHEDULE OF PRICES

Bids offered are f.o.b. destination.

Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications.

Bidder must make an entry in each of the spaces provided. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids may be declared nonresponsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government.

Bids submitted with NB (No Bid) or blank spaces for an item may be declared nonresponsive.

The Contracting Officer reserves the right to reject any offer that contains prices for individual items of production (whether or not such items are included in the Determination of Award) that are inconsistent or unrealistic in regard to other prices in the same offer or to GPO prices for the same operation if such action would be in the best interest of the Government.

Fractional parts of 1,000 will be prorated at the per 1,000 rate.

Invoices submitted to GPO by contractor must have line-item pricing identified using the same outline numbering format used for the "Schedule of Prices" in the contract specifications. Each line-item must be been labeled with the outline number of the corresponding task/item specified in the "Schedule of Prices" (for example: II. (a).1).

Prices must be submitted for the entire term of the contract and bids qualified for a lesser-period will not be considered.

Prices must include any corrections/adjustments to the files, requested from the customer after the initial review.

I. MAIL FILE PROCESSING:	(1) up to 20,000 Records	(2) 500,000 to 10,000,000 Records	(3) 10,000,001 to 41,000,000 Records
a. CASS/NCOA Processing ...per 1,000 records...	$ _____	$ _____	$ _____
b. Deceased Coding ..... per 1,000 records input ...	$ _____	$ _____	$ _____
c. Deceased Coding ...per 1,000 records matched ..	$ _____	$ _____	$ _____
d. Apartment Append .... per 1,000 records input ..	$ _____	$ _____	$ _____
e. Apartment Append.. per 1,000 records matched ..	$ _____	$ _____	$ _____
f. De-Duping ..... per 1,000 records input ..	$ _____	$ _____	$ _____

II. ADDITIONAL OPERATIONS

a. System Time Work ..... per hour ..... $ _____
(System Time Work must be pre-approved by customer agency)

_____
Initials

INSTRUCTIONS FOR BID SUBMISSION: Fill out "Section 4.- Schedule of Prices", initialing or signing each page in the space(s) provided. Submit two copies (original and one exact duplicate) of the "Schedule of Prices" with two copies of GPO Form 910, "BID" form. Do not enter bid prices on GPO Form 910; prices entered in the "Schedule of Prices" will prevail.

Bidder _____

_____
(City - State)

By _____
(Signature and title of person authorized to sign this bid)

_____
(Person to be contacted) (Telephone Number)

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, *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.

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:

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:

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.

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.

This page deliberately left blank.

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)*

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	19. POSITION SENSITIVITY LEVEL
20. ID BADGE EXPIRATION DATE *(mm/dd/yyyy)*	☐ Non-Sensitive (1) ☐ National Security/Secret or Confidential (2) ☐ National Security/Top Secret (3) ☐ National Security/Top Secret - SCI (4) ☐ Public Trust/Moderate Risk (5) ☐ 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.

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.

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)*

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

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

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

File	Years(s)	System of Record

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	

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

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0734. The time required to complete this information collection is estimated to average 30 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: Reports Clearance Officer, Baltimore, Maryland 21244-1850.

Form Approved
OMB No. 0938-0734

ADDENDUM TO DATA USE AGREEMENT (DUA)

Addendum to DUA for _____. If this is an addendum to a previously approved DUA, insert the CMS assigned DUA number here: _____. The following individual(s) may/will have access to CMS data that is being requested for this agreement. Their signatures attest to their agreement to the terms of this Data Use Agreement:

Name and Title of Individual *(typed or printed)*		
Task / Role of this individual in this project	Company / Organization	
Street Address		
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
Signature of Individual	Date	
Signature of CMS Representative	Date	
Signature of CMS Project Officer *(If applicable)*	Date	

Name and Title of Individual *(typed or printed)*		
Task / Role of this individual in this project	Company / Organization	
Street Address		
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
Signature of Individual	Date	
Signature of CMS Representative	Date	
Signature of CMS Project Officer *(If applicable)*	Date	

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0734. The time required to complete this information collection is estimated to average 30 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: Reports Clearance Officer, Baltimore, Maryland 21244-1850.

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

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-1046. The time required to complete this information collection is estimated to average 10 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, Maryland 21244-1850.

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

Secure One HHS

Information Security Program Rules of Behavior

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

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

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

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

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

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

- Information and system use must comply with Department and OPDIV policies and standards, and with applicable laws.
- Use for other than official, assigned duties is subject to the HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources, dated February 17, 2006.

- Unauthorized access to information or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII)[3]

Users shall:

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

Users shall **not**:

- Direct or encourage others to violate HHS policies.
- Circumvent security safeguards or reconfigure systems except as authorized (i.e., violation of least privilege).
- Use another person's account, identity, or password.
- Remove computers or equipment.
- Send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums.
- Exceed authorized access to sensitive information.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on portable devices such as laptops, personal digital assistants (PDA) and universal serial bus (USB) drives or on remote/home systems

without authorization or appropriate safeguards, as stipulated by the HHS Encryption Standard for Mobile Devices and Portable Media, dated August 21, 2007.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others. (See 18 U.S.C. 2071)
- Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without permission or license from the copyright owner.
- Modify software without management approval.

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

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

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

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

Users shall ensure that passwords:

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

SIGNATURE PAGE

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

Signatures: _____

Date Signed: _____

Employee's/User's Name: _____

(Print)

APPROVED BY AND EFFECTIVE ON:

/s/ February 12, 2008

Michael Carleton
HHS Chief Information Officer

DATE

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