EUA WorkFlow Request No.

APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS

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

❏ NEW *(Issue a CMS UserID)*

❏ CONNECT/DISCONNECT
(Add/remove access authorities)

❏ CERTIFY *(Due date: ____/_____)*
          mo   yr

❏ CHANGE USER INFORMATION *(Note new info)*

❏ DELETE *(Remove CMS UserID from all CMS systems)*

USERID
(Capital Letters)

2. USER INFORMATION

❏ CMS Employee
❏ Medicare Advantage / Medicare Advantage with Prescription Drug / Prescription Drug Plan / Cost Contracts – Using HPMS Only
❏ Medicare Advantage / Medicare Advantage with Prescription Drug / Prescription Drug Plan / Cost Contracts – Using Other Systems
❏ CITIC Contractor
❏ Program Safeguard Contractor
❏ Medicare Contractor/Intermediary/Carrier
❏ Contractor (non-Medicare contract with CMS)
❏ Researcher
❏ Quality Improvement Organization
❏ End-Stage Renal Disease Network
❏ State Agency (State of _____)
❏ Federal Govt – Baltimore HR Center

❏ Federal Govt – Centers for Disease Control & Prevention
❏ Federal Govt – Commission Corps
❏ Federal Govt – Dept of Health & Human Services
❏ Federal Govt – HHS – OMHA
❏ Federal Govt – Dept of Justice
❏ Federal Govt – Dept of Veterans Affairs
❏ Federal Govt – Government Accountability Office
❏ Federal Govt – General Services Administration
❏ Federal Govt – Internal Revenue Service
❏ Federal Govt – Office of General Counsel
❏ Federal Govt – Office of Inspector General
❏ Federal Govt – Railroad Retirement Board
❏ Federal Govt – Social Security Administration
❏ Federal Govt – Other: _____
❏ Other: _____
_____

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

Company/Organization/Department Name

Mailing Address *(Include Suite/Mailstop)*

City | State | ZIP Code

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

IF CMS EMPLOYEE Org Name/Admin Code | Are you a Manager? ❏ Yes ❏ No

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

❏ R4 (AFC) Atlanta
❏ R10 (BLNCH) Seattle
❏ CO (CENTRAL) Central Office
❏ R5 (CHIICB) Chicago
❏ DC (COHEN) DC
❏ R6 (DAL1301) Dallas
❏ R8 (DENCSB) Denver
❏ R7 (FOBKAN) Kansas City

❏ DC (HHH) DC
❏ R9 (HWTHRN) San Francisco
❏ R1 (JFKBOS) Boston
❏ R2 (JKJNYC) New York
❏ CO (LBDCO) Central Office
❏ CO (NORTH) Central Office
❏ R3 (PHIPLB) Philadelphia
❏ CO (SOUTH) Central Office
❏ Other _____

Mail Stop | Desk Location

3. WORKLOAD INFORMATION

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

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

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

Grant Number *(for Researchers)*

Inter-Agency Agreement Number

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

❏ Connect ❏ Disconnect ❏ Keep **Default CMS Employee** (standard desktop & network with CMS e-mail acct)

❏ Connect ❏ Disconnect ❏ Keep **Default Non-CMS Employee** (standard network access)

❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____

❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____
❏ Connect ❏ Disconnect ❏ Keep _____

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

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

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

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

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

Printed Name		Telephone Number	
CMS UserID	Signature		Date

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

Printed Name		Telephone Number	
CMS UserID	Signature		Date

APPLICANT: Read, complete and sign next page.

APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS

Printed Name *(As you want it published)*

Social Security Number

CMS USERID

PRIVACY ACT STATEMENT

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

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

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

SECURITY REQUIREMENTS FOR USERS OF CMS COMPUTER SYSTEMS

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

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

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

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

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

Applicant's Signature

Date