QIES Business Intelligence Center Access Request Form

Type of Request

☐ New User ID ☐ Change Access ☐ Change Organization ☐ Delete User ID

EIDM/QARM User ID:

Requester Information

Requester Name: Title:
Last, First, Middle Initial

Organization:

User Location: City: State:

Work Phone Number: Extension:

Work E-mail Address:

Type of User: ☐ CMS ☐ Regional Office ☐ State Survey Agency ☐ QIO/QIN

☐ Contractor Type:

☐ Other:

DUA Number: DUA Expiration Date: Carrier Number (MAC Only):

QBIC Data Access

☐ MDS QI ☐ OBQI ☐ Survey and Certification (Includes Provider/Enforcement (AEM) and CLIA data)

☐ MDS NH Assessment ☐ MDS SB Assessment ☐ OASIS Assessment ☐ IRF-PAI Assessment ☐ LTCH Assessment ☐ Hospice Assessment ☐ ACTS ☐ PBJ

Other Access

☐ RHHI Extract ☐ MDS NH Extract ☐ MDS SB Extract ☐ IRF-PAI Extract

Access to States: Request Date:

Other Access Not Listed:

Business Need for the Requested Access:

CMS Authorization - Required for Approval

This section is completed by CMS

CMS Authorizer Type: ☐ CMS Regional Office ☐ CMS Central Office

Approved QBIC User Role: *(Choose only one)* ☐ Ad Hoc ☐ Report Submitter Only

Approved QBIC Admin Roles:

CMS Authorizer Name: CMS Authorizer Signature: (sign in black or blue ink)
Last, First, Middle Initial

CMS Authorizer Phone: Ext: Date:

PRIVACY ACT ADVISORY STATEMENT

Privacy Act of 1974, P.L. 93-579

The information on side 1 of this form is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10). 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 stature, 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 System 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.

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 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 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 will 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 sub files 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 someone else may have used your identification number or password, immediately report that information to your security officer.

Signature of User: (sign in black or blue ink) Date:

_____ _____

Printed User's Name:

_____