

# EPOC ACCESS ACKNOWLEDGEMENT FORM

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

- NEW EPOC Designation                       CERTIFY
- DISCONNECT EPOC Access

## 2. USER INFORMATION

User ID

First Name *(As you want it published)*

MI

Last Name *(As you want it published)*

CompanyName

Mailing Address *(Include Suite/Mailstop)*

City

State

ZIP Code

Office Telephone *(Include Extension)*

Company Telephone *(If different)*

E-Mail Address

## 3. WORKLOAD INFORMATION

Contract Number(s)

## 4. JUSTIFICATION

## 5. APPROVALS:

### PROVIDE SIGNATURES BELOW

**Authorization:** We acknowledge that our Organization is responsible for all resources to be used by the person identified above and the requested access is 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 email request.

### 1st APPROVER *(Company Official authorized to designate a plan EPOC)*

Printed Name

Telephone Number

Signature

Date

### 2nd APPROVER *(CMSEPOC Authorizer)*

Printed Name

Telephone Number

Signature

Date

**APPLICANT:** Read, complete and sign following pages.

---

## **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.

---

## EPOC REQUIREMENTS

Signing and submission of this form is considered acceptance of the following policies below:

- Plans and EPOCs are required to establish a procedure for reviewing end user access twice a year. EPOCs are responsible for removing access from any user who no longer requires access to the MARx system to perform job duties, has separated from the company or who has not accessed the system.
- EPOCs are required to complete certification on all end users under his/her authority annually. Part of the certification process is to verify each user should remain active in the MARx system for all respective contracts under his/her ID. If an EPOC chooses to bulk approve users, the EPOC is certifying that he/she did a review on each user and the access to those contracts should remain. Any certifications not completed by the deadline will result in a user losing access to those contract associated to his/her account. No extensions will be given to EPOCs as non-completion of annual recertification on time is a security violation.
- EPOCs are required to submit EPOC Designation Letters and a signed EPOC Access Acknowledgement form on an annual basis to CMS. This will justify continued EPOC access to the designated contracts during annual certification.

---

Printed Name *(As you want it published)*

---

Date

---

Applicant's Signature

---

Date
------