AHIN | PRO Medicare System Access Enrollment Form

Organization Information		Organization IT Information	
Name:		Technical contact:	
Phone Number:		Phone Number:	
Address 1:		Email Address:	
Address 2:		Please email or fax to: APSenrollment@AHIN.net Fax: 501-378-2484 Any questions call us at 855-822-AHIN	
City:			
State, Zip code:			
Email Address:			

Additional Organization Information		Medicare System ACCESS	
Medicare Group NPI:			
Medicare PTAN:		Select Service:	o PPTN
EIN:			o HETS
AHIN Submitter ID:			o FISS

In order to be setup for Medicare Access AHIN will need the sourced IP address of the user(s). If you have a firewall this will be the IP address facing the internet. If you do not use a firewall contact your Internet Service Provider to obtain your IP. While there is not a setup fee associated with Medicare System Access if you do not provide the correct IP information and we have to have a technical call to facilitate connectivity there will be a $50.00 per hour fee added to your account for the first month's billing. Sourced IP address: _____

It is the responsibility of the facility to request FISS or PPTN user ID's, passwords, and PINS from your Medicare Administrator Contractor (MAC). APS cannot obtain this information for you. APS only provides connectivity to CMS Systems and cannot reset a user's CMS account this can only be done by your MAC.

List all users that need to have Medicare System Access

First Name:	Last Name:	Date of Birth:
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Internal use only: Date Firewall setup for Sourced IP_____			
Date received :	Date Setup completed:	Date Provider notified of go live:	Setup by:
AD Server Setup:	AD Server PIN:	AHIN Temp PIN:	Facility setup AD Date: Date completed setup:
User 1 ID:			
User 2 ID:			
User 3 ID:			
User 4 ID:			
User 5 ID:			
User 6 ID:			

AHIN | PRO

CMS ACCESS TO COMPUTER SYSTEMS PRIVACY STATEMENT

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.

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, remove or transmit data unless you have been specifically authorized.
- 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 known.
- 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:

The signature above is legally authorized and approved by an organization to agree to all CMS System Access requirements.