CMS Response to Public Comments Received for CMS-10220

The Centers for Medicare & Medicaid Services (CMS) received comments from the public regarding a new information collection instrument, CMS-10220. This is the reconciliation of the comments.

Comment:

One commenter stated that *"to date, no information has been shared with providers regarding this process, nor has the provider community's input been sought in the development of this system."*

Response:

CMS is currently in the process of coordinating plans for public education and outreach. Our activities will include User Acceptance Testing (UAT) and the development of public outreach materials.

Comment:

One commenter stated that *"Generally, employment contracts with practitioners contain a provision granting the medical practice and appropriate staff permission to complete the necessary credentialing applications on their behalf. Therefore, this proposed PECOS Web Security Consent form is duplicative and unnecessary."*

Response:

CMS appreciates concerns expressed by the commenter, but we disagree that the Security Consent form is duplicative and unnecessary. Authorization is required through the Security Consent form for a PECOS Web user to perform Medicare enrollment activities on behalf of a provider and to view their existing enrollment data which could consist of Privacy Act-protected or other sensitive data.

The form once signed, mailed and approved, grants the user access to the Medicare enrollment records of the specified provider.

Comment:

Two commenters suggested that CMS reduce the number of Security Consent Form versions from four to two; one for individuals and one for groups.

Response:

CMS agrees with the commenter and will reduce the number of Security Consent forms. Specifically, we will create a single Security Consent form for individuals and organizations.

Comment:

One commenter stated that *"It is unclear from the proposed versions of the PECOS Web Security Consent form, however, whether each individual user will need to have a separate consent form signed by each provider or if individuals signing Sec. 2B will be able to designate and provide access to the appropriate staff members without separate and distinct notifications to CMS."*

Response:

Only one Security Consent form per user group is required to be signed that will grant the user group and its associated users' access to all current and future enrollment data for the specific Medicare provider and to submit enrollment data. Each individual and organization provider would have to sign a Security Consent form to enable a user group to submit or view its enrollment data via PECOS Web

Comment:

One commenter suggested that "the term Medicare Identification Number" be expanded to include the NPI and that CMS link access to enrollment applications together by NPI. It was also suggested that space be provided for more than four Medicare identification numbers or that an instruction be added and attachments be accepted.

Response:

CMS agrees with the commenter and has removed the term "Medicare Identification Number" from the Security Consent forms. The user group and its associated users will now have access to all current and future enrollment data for the particular Medicare provider, not only to enrollment data linked to specific Medicare identification numbers.

Comment:

One commenter stated that the term "Application Tracking ID" is not defined in the initial version of the proposed PECOS Web Security Consent forms and request that CMS clarify this term.

<u>Response:</u>

The application tracking ID is a system generated number and will appear on the Security Consent form that all other attachments when printed. Its purpose is to track and link the hard copy attachments with the enrollment data submitted electronically via PECOS Web to the Medicare contractors. An application tracking ID itself does not convey access to a provider's enrollment data by a user group.

We will clarify this term is our education and outreach material.