

Comments to Centers of Medicare and Medicaid Services

December 22, 2017

Proposed rule to revise the Medicare Advantage program (Part C) regulations and Prescription Drug Benefit Program (Part D) regulations

File code CMS-4182-P

Respectfully submitted by: Michael Laurie, Vice President, Product Strategy, eSignLive by VASCO

Michael Magrath, Director, Global Regulations & Standards, VASCO

**Identity of Healthcare Providers (Page 122)**

***In paragraph (c)(5)(v), we state that with respect to requests for reimbursement submitted by Medicare beneficiaries, a Part D sponsor may not make payment to a beneficiary dependent upon the sponsor's acquisition of an active and valid individual prescriber NPI, unless there is an indication of fraud. If the sponsor is unable to retrospectively acquire an active and valid individual prescriber NPI, the sponsor may not seek recovery of any payment to the beneficiary solely on that basis.***

The U.S. Drug Enforcement Administration’s 2010 Rule for Electronically Prescribing Controlled Substances defines identity proofing requirements for DEA Registrants (providers) which includes in-person identity proofing involving checking identity documents such as a driver license and/passport. Additionally, providers could be identity proofed remotely by answering a series of questions that should be known only to them typically based on information contained in one’s credit report. This is known as knowledge based verification (KBV). KBV was not an optimal solution since passing the questions is based on a combination of accuracy and timing. Additionally the credit reporting agencies do not have data on 100% of the healthcare providers. Since then there have been widescale cyber attacks across many industries, including healthcare. These attacks have compromised personally identifieable data on millions of Americans leaving the viability of KBV identity proofing in question. Should CMS continue to use KBV it should be augmented with other means as part of a risk based approach.

Much has changed since 2010. Biometric enabled smartphones are in the hands of millions and can be used as part of a robust identity proofing process and for multi-factor authentication.

HIMSS formed the Identity Management Task Force focuseD on policy and technical challenges relating to identity, attribute and role based access management, as it pertains to patient identity, provider identity and IT asset identities. The Task Force published “Patient Portal Identity Proofing and Authentication” in 2016. The task force published identity proofing and authentication recommendations for patients accessing their health information electronically. Included in the guidance are discussions about how to conduct identity proofing and authentication at a high level of confidence, how to handle delegating access to patient information and addressing situations where a user would like to remain anonymous. Although paper defines best practices for patients, it leverages existing NIST guidance for identity proofing and authentication and many of the uses cases are applicable to providers and CMS should review them.

Additionally, NIST updated its Digital Identity Guidelines over the summer of July 2017. NIST Special Publication 800-63A, “Digital Identity Guidelines: Enrollment and Identity Proofing” should be considered by CMS as it relates to identity proofing providers. Included is acceptance of virtual in-person identity proofing, which requires an individual to be interviewed by a trained agent via a video conference call that is time stamped and recorded to provide an audit trail and archive.

**Electronic Signature (Page 139)**

***To address concerns from providers about burdensome requests from MA organizations for their patients' medical record documentation, we are soliciting comment from stakeholders to more fully understand the issue and for ideas to accomplish reductions in provider burden.***

The following comments address whether there is reduced burden associated with electronic signatures in relation the nature and extent of requests related to medical record attestations.

Medical record attestation requests are required when the handwritten signature of a health care provider is illegible or missing from a medical record required under CMS. Under CMS, a health care provider may use a handwritten signature or an electronic signature and the attestation is required in the case of the former.

Electronic signatures are widely used today in many regulated industries that include health care, insurance, banking, life sciences, as well as by all levels of government. Health care providers have been adopting and using electronic signature since they were sanctioned by HIPAA.

Since the health care provider has the choice, using a well-designed, HIPAA-compliant electronic signature solution such as eSignLive by VASCO should be considered for the following reasons:

1. An electronic signature is represented by a secured image in the PDF document indicating the name of the person, the signing date and time in an easily legible font. The signature block is also clickable to view a secure, embedded audit trail that is part of the electronic document. This ensures that the information about who signed, when and why is clearly preserved in the document which eliminates the possibility of an illegible signature.
2. The placement of an electronic signature is assured since once the signer is authenticated to access the document through a web browser, they are directed to the place where the electronic signature is to be placed. If the signing is not completed, reminders can be sent to the signer to complete the e-signing. The signing can also be part of a workflow to further assure the completion of the signing process. As a result, placing of an electronic signature will not be overlooked by the health care provider.
3. In addition to the electronic signature, other required data can be added automatically to the form with the electronic signature such as location, name of health care organization, and other identifiers. Again, this automation ensures that the form is properly completed.
4. A number of authentication options are available for the signer that range from a user ID with PIN to two-factor authentication through the signer’s mobile device. An appropriate level of authentication can be selected to ensure that the form was only signed by the authorized health care provider.

The advantages of a well-designed electronic signature system have been shown to substantially reduce errors when compared to manual, paper-based signing procedures. Since attestations are the result of erroneously signed records, the use of electronic signatures would assist in reducing the number of attestations.