EPCS Compliance for Cerner Millennium and PowerChart Ambulatory

with VASCO Two-Factor Authentication

- **Satisfies DEA's Requirements for Electronic Prescription of Controlled Substances (EPCS)**
- **Maintains existing provider workflow**
- **FIPS compliant**
- **Helps ensure HIPAA, and Meaningful Use compliance**
- **Natively integrated with Cerner's Millennium®, PowerChart® Ambulatory.**

WHY YOU NEED TWO-FACTOR AUTHENTICATION FOR YOUR CERNER MILLENNIUM SYSTEM?

DEA regulations mandate the use of two-factor authentication when a prescription for a controlled substance is submitted electronically. That means that all EPCS enabled electronic prescribing systems must support such technology and all authorized prescribers (such as physicians and nurse practitioners) must be equipped with appropriate security tools. In practical terms, all users of Cerner Millennium that wish to prescribe controlled substances electronically need to possess one of the two-factor authentication tools/devices as required by the DEA.

WHAT IS TWO-FACTOR AUTHENTICATION?

Two-Factor Authentication (or frequently referred to as multi-factor authentication) is a method of verifying a user's identity electronically that requires at least two elements. Simply put, it's using a combination of at least two factors to prove that you are who you claim to be:

- **Factor 1 – Something you know.** Your user name and regular static password or PIN.
- **Factor 2 – Something you have.** A one-time password (a 6-digit code) generated by your hardware or software token.
- **Factor 3 – Something you are.** Biometrics.

Two-factor authentication is required when prescribing controlled substances electronically at all times. The combination of a user ID and password is considered to be only one factor, because it requires only information that a user knows, so that's not sufficient.

In order to be compliant with EPCS, authentication credentials must be SEPARATE from the device used to access the e-prescribing application. So if you're prescribing from a mobile device, and you're using a software authenticator on that device, you are NOT in compliance. A FIPS 140-2 compliant (or Federal Information Processing Standard) hardware OTP token will ensure that authorized prescribers can use both PC and mobile applications.

Multi-factor authentication – "best practice" for risk mitigation according to Department of Health and Human Services

Two-factor authentication is required by DEA for EPCS

Prevents many data breaches. Two-factor authentication gives your organization an additional layer of security when accessing PHI and helps your organization comply with the Technical Safeguards defined in the HIPAA Security Rule. Two-factor authentication devices generate one-time passwords (OTPs) that augment the commonly used, insecure static user name/password combination thus rendering hacker attacks infective.

No more password reset calls to your helpdesk! Two-factor authentication will significantly reduce "forgot-my-password" calls and help reduce associated costs

VASCO DIGIPASS FOR CERNER MILLENNIUM

Cerner and VASCO Data Security have partnered to deliver a compliant and secure solution to Cerner customers in the most convenient way. VASCO authentication technology has been natively integrated in Cerner Millennium to maintain existing workflows and minimize additional steps and integration debacles.

Cerner is now a Value Added Reseller of VASCO's two-factor authentication solutions including:

- Hardware authentication "tokens"
  - DIGIPASS GO7 – one-button, FIPS compliant device
  - DIGIPASS 270 – PIN protected for added security
- Mobile authenticators
  - DIGIPASS for Mobile – FIPS certification pending*

HOW IT WORKS - AT LOGIN

Within Millennium, applications can require two-factor authentication upfront when the user first logs in.

HOW IT WORKS - AT WORKFLOW

The application can require two-factor authentication only during certain workflows within the application, such as when a provider is prescribing a controlled substance or when the provider is viewing sensitive data, such as data derived from Medicare/Medicaid claims.

This "step-up" authentication allows added usability and only requests two-factor authentication when the application requires it and, in addition, does not overload the user by having to enter subsequent consecutive requests for authentication.

WHY VASCO?

No additional development work - take advantage of the native integration. Cerner has done all development work so you don't have to, drastically reducing the cost and complexity of implementation and support. With no need for additional databases or servers, you can get up and running quickly, and with minimal resources.

Guaranteed Compliance – VASCO offers the only one-time password OTP hardware token that is FIPS 140-2 Level 2 Certified and satisfies the DEA requirements for EPCS. Mobile token certification is pending*.

Fully Scalable - VASCO's DIGIPASS authentication technologies can accommodate as few as two or as many as 100,000+ users—all on the same backend platform and without any overhaul in infrastructure. All you need to do is to purchase additional licenses and authenticators.

Long-term Savings – VASCO's FIPS Compliant DIGIPASS GO7 token has an average life span of 10+ years and no artificial expiration date.

WHERE TO BUY

Cerner is an official Value Added Reseller of VASCO two-factor authentication products. Please contact a VASCO representative or your Cerner customer care representative for more information and a quote.

*Certification expected July 2017.

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications, and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets. Learn more about VASCO at vasco.com and on Twitter, LinkedIn and Facebook.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

DS-2016011