surescripts
The Nation's E-Prescription Network

Surescripts Position Regarding Drug Enforcement Administration (DEA) Electronic Prescribing for Controlled Substances (EPCS) Third-Party Audit Requirements
October 31, 2012

According to the DEA's EPCS interim final rule (IFR) published in the Federal Register on 03/31/2010 (effective 06/01/2010), in order for a prescriber or pharmacy application to be used for EPCS purposes (emphasis added):

> "… the application provider of an electronic prescription application or a pharmacy application must have a third-party audit of the application that determines that the application meets the requirements of this part at each of the following times: (1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions." [21 CFR Part 1311.300(a)]

Recently, it has come to Surescripts' attention that the following statements have been made within the industry:

> "… end-users… must have their security practices approved…" and "… each hospital in a multi-hospital system, each medical office in large group practice and each store location in a pharmacy chain would need to participate in the security assessment."

These statements have started to generate confusion and concern among industry stakeholders, physician and pharmacy application vendors, and their end users, so Surescripts would like to take this opportunity to point out that neither the DEA's EPCS IFR, nor subsequent published guidance, makes any such requirements on end-user hospitals, physicians or pharmacies. According to the DEA's rule quoted above, the only specific audit requirements described in the rule apply to EPCS applications used by prescribers and pharmacies. Thus, it is Surescripts' position that the purported end-user requirements mentioned above are not supported by applicable laws or regulations.[1] Should a physician or pharmacy application vendor be told by a potential Part 1311 EPCS auditor that end-user approvals would be required by said auditor as part of its EPCS audit process, Surescripts suggests that the vendor consider investigating the services of other auditors that meet the DEA's criteria, as there clearly are auditors in the marketplace that make no such requirements on end users.

Although Surescripts does not recommend or endorse auditors to its network participants as being able to conduct EPCS audits, to assist its participants in evaluating

[1] Surescripts does not provide legal advice, and nothing herein should be construed as legal advice. Participants are encouraged to consult with legal counsel regarding their obligations under law.

2800 Crystal Drive
Arlington, VA 22202
T: 866.797.3239 F: 877.801.2536

www.surescripts.com

920 2nd Avenue South
Minneapolis, MN 55402
T: 866.267.9482 F: 651.855.3001

the many potential auditors that are available, Surescripts is willing to share information that has been reported to it by its network participants that have completed or are currently undergoing EPCS audits. As a reminder, according to the DEA EPCS IFR and the DEA clarification/notification statement released on 10/14/2011:

> "There are two alternative processes for review of EPCS applications: (1) A third-party audit conducted by a person qualified to conduct a SysTrust, WebTrust or SAS 70 audit or a Certified Information System Auditor as stated in 21 CFR 1311.300(b), which comports with the requirements of paragraphs (c) and (d) of 21 CFR 1300.300 or (2) A certification by a certifying organization whose certification process has been approved by DEA as stated in 21 CFR 1311.300(e), which certification verifies that the application meets all of the requirements of 21 CFR Part 1311."

The DEA now lists organizations in the second of these categories on its website at http://www.deadiversion.usdoj.gov/ecomm/e_rx/thirdparty.htm#approved, but the DEA has not posted the names of any organizations that belong in the first category. To address this information gap, Surescripts is sharing the following names of organizations that network participants have reported they have used for EPCS audits. It is our understanding that these organizations belong in one or more of the categories recognized by the DEA as being able to perform EPCS audits, i.e., SysTrust, WebTrust, SAS 70 and/or Certified Information System Auditors (CISAs):

- Assurance Concepts, LLC
- BDO USA, LLP
- BrightLine
- Chief Security Officers, LLC
- ComplySmart, LLC
- Deloitte & Touche LLP
- Electronic Healthcare Network Accreditation Commission (EHNAC)
- Ernst & Young LLP
- KPMG LLP
- McGladrey & Pullen, LLP
- NetSPI
- Price Waterhouse Coopers

Again, Surescripts does not recommend or endorse any of these specific companies over another, and this list should not be considered to be comprehensive. It is simply meant to provide examples of the types of firms that are offering EPCS audit services in the industry. This said, it is Surescripts' understanding that processes and pricing vary greatly among these many potential audit organizations, so network participants are encouraged to shop and compare before contracting with any such companies.