HIMSS Analytics

HIMSS Analytics Stage 7 Case Study

Cambridge Health Alliance

Profile

CHA is a three-hospital system based in Cambridge, MA. CHA acts as the Cambridge Public Health Commission and Public Health Department of the City of Cambridge and serves as a teaching hospital for Harvard University and Tufts University. CHA employs 4,323 staff, including 690 physicians, and serves more than 140,000 patients in Boston's Metro North region. CHA has received NCQA Level 3 Medical Home recognition for ten of its twelve primary care practices, achieved HIMSS Stage 6 for Acute and Ambulatory in May 2015, and HIMSS Stage 7 for Ambulatory in September 2015.

The Challenge

Cambridge Health Alliance (CHA) deployed electronic prescribing of controlled substances (EPCS) to improve patient care, address clinical workflow inefficiencies, and protect against prescription fraud. This paper outlines CHA's drivers for implementing EPCS and shares the lessons CHA learned during their EPCS deployment processes, offering best practice advice for hospitals who are interested in achieving EPCS success.

Implementation Overview

EPCS
Electronic Prescribing of Controlled Substances (EPCS) was legalized by the DEA in 2010. EPCS enables prescribers to send electronic prescriptions of controlled substances directly to patients' pharmacies. EPCS eliminates the need for doctors to write or print paper scripts, for patients to carry paper scripts with them to their pharmacy, and for patients to wait extra time while their prescription medications are being processed. Due to the highly powerful and addictive nature of controlled substances, EPCS requires additional security measures above and beyond those required for regular e-prescribing. The DEA requires care providers to complete two-factor authentication for EPCS order signing and provides detailed rules and regulations for provider identity-proofing, credential enrollment, and auditing and reporting requirements to ensuring the authentication of EPCS orders is secure and legitimate. These security measures are designed to protect against prescription fraud and doctor shopping in an effort to address the growing prescription drug abuse epidemic that claims more lives in the U.S. every year than heroin and cocaine abuse combined.

Motivating factors: Why CHA chose EPCS

- To increase patient safety and satisfaction

EPCS improves patients' prescription experiences by automating the prescription process and saving patients considerable amounts of time. With EPCS, patients no longer need to travel to their pharmacy and wait while their prescription is being processed. Instead, their prescription is directly sent to their pharmacy electronically, allowing patients to reclaim the time they previously spent manually delivering prescriptions. Improving patients' prescription experiences and expediting patients' access to critical pain medications was an important factor in CHA's decision to implement EPCS because CHA caters to a particularly socio-economically disadvantaged patient population who depend on public transportation. By reclaiming patients' time waiting at pharmacies and reducing patients' travel times between different clinics to pick up refill orders, CHA reduces disruptions to for patients and improves their experience. "It can really by life--changing for our patient population to get their care effectively, quickly, and with minimal interruption to their day and their lives," says Arthur Ream III, Director of IT Applications and CISO of CHA.

- To improve provider satisfaction and efficiency

EPCS enables physicians to use the best technological tools available to improve their efficiency and eliminate frustrating dual prescribing workflows. Before enabling EPCS, CHA had two prescribing systems: an e-prescribing system for non-controlled substances and paper-based prescriptions for controlled substances. Whenever doctors had to write combined prescriptions including both controlled and non-controlled substances, they had to perform two separate prescription processes. Or, they simply opted to prescribe all substances via a paper to save time and improve efficiency. This cumbersome dual prescribing workflow caused frustration for clinicians, increased wait times for patients at pharmacies, introduced the risk of drug diversion and fraud, and posed a threat to achieving Meaningful Use e-prescribing targets. By adopting EPCS, CHA's prescribers have a simplified, consistent workflow for all prescriptions. Since implementing EPCS, CHA has increased overall e-prescribing utilization for both controlled and non-controlled substances by 40 percent, helping to meet Meaningful Use criteria.

- To join Massachusetts' leaders in the effort to combat prescription fraud and abuse

In June 2015, a task force assigned by Massachusetts Governor Charlie Baker outlined a series of recommendations, including increased use of EPCS, to reverse the trend of opiate abuse and addiction that claimed the lives of more than 1,000 Massachusetts residents in 2014. CHA wanted to help change these trends by becoming an early adopter of EPCS, leading the way in Massachusetts' efforts to combat prescription drug abuse and improve patient safety. "As part of a robust strategy to curb prescription drug abuse, we need to give providers the best tools available to help them make sound decisions when prescribing controlled substances. We view EPCS as essential because it greatly reduces the risk of fraud and drug diversion while also ensuring that patients with chronic pain can more easily get the medications they need," says Ream.

Deployment best practices

- Perform a thorough assessment of your technology landscape:

Ream and his staff began CHA's EPCS project with a thorough assessment of CHA's technology environment and Epic EMR system. CHA was already using Surescripts and VIP Symantec tokens for e-prescribing non-controlled substances, so Ream decided to seek out technology vendors who offered EPCS solutions that worked well with Epic, Surescripts, and Symantec. CHA's Implementation Team included Epic Analysts, Systems and Server experts, a System Engineer for Desktop Services, and contacts from Surescripts and Epic.

- Actively involve your Clinical Informatics team to meet your clinicians' needs:

CHA's EPCS project was spearheaded by the IT and Implementation teams, but it could not have been thoroughly successful without IT collaborating with CHA's Clinical Informatics Group. Ream collaborated directly with CHA's CMIO, Chief Nursing Information Officer, and a cohort of Informatics in the Analytic Team. "One of my main pieces of advice is that it's important to engage your clinical informatics folks," says Ream. "They practice every day, provide invaluable feedback for pilot projects, and know exactly what user requirements technologies need to succeed in the clinical environment."

- Decide whether institutional or individual identity proofing is right for your organization

The DEA requires care providers to complete an identity proofing process before they can be enabled for EPCS. This step ensures the provider is authorized to prescribe controlled substances and is given the necessary credentials to be enrolled in an EPCS system. The DEA allows both institutional and individual identity proofing, and as one of the first steps in the EPCS enablement process, organizations must decide which option is best for them. Here is an overview of each:

- Institutional identity proofing is typically done through an organization's internal credentialing office, which undergoes the process of verifying the identities of all prescribers to be enrolled in the organization's EPCS system. For an organization to use institutional identity proofing, it must have an institutional DEA number.

- Individual identity proofing is carried out by the individual providers using a third-party credentialing service provider (CSP) such as Symantec.

The provider must give the CSP sufficient documentation of their identity, and if they are successful, they will be issued credentials (for example, a token) confirming their completion of the identity proofing process. If an organization does not have an institutional DEA number, it must opt for individual identity proofing. However, it is important to note that even if organizations are eligible for institutional identity proofing, they can opt for individual identity proofing (for instance, if the credentialing office is understaffed or if the health system has many remote providers).

Resulting Value / ROI

- Choose an EPCS partner that works well with your existing technology base and offers robust interoperability and user options:

To ensure the success of CHA's EPCS project by enabling clinicians with the most flexible, interoperable, and secure solutions for meeting DEA requirements for EPCS while ensuring fast, convenient workflows for clinicians. To complement CHA's existing Epic and Symantec technologies and provide the most flexible two-factor authentication modalities for prescribers, Ream selected Imprivata Confirm ID.

Imprivata Confirm ID is the fast, secure signing solution for EPCS. Imprivata Confirm ID is the industry's most comprehensive platform for meeting the provider identity-proofing, credential enrollment, two-factor authentication, and auditing and reporting to streamline compliance with the DEA requirements for EPCS. Imprivata Confirm ID also simplifies EPCS for providers by integrating with leading EMRs and e-prescribing applications and offering the broadest range of two-factor authentication modalities to give providers the necessary flexibility to leverage the authentication options that best meet their prescribing workflow requirements.

This includes Hands Free Authentication, a breakthrough, proximity-based authentication solution that delivers exceptional speed, security, and convenience for providers. Hands Free Authentication wirelessly retrieves and verifies a passcode from a user's mobile device, even if it is locked, without requiring the provider to enter a passcode or type a one time passcode (OTP) from a token. This process delivers unparalleled speed and convenience that minimizes impact to clinical workflows and increases provider satisfaction.

Ream chose Imprivata Confirm ID because of the breath of two-factor authentication options it supports. Ream was particularly impressed by Hands Free Authentication's ability to meet the user needs outlined by his Clinical Informatics team. "Hands Free Authentication is the key to maintaining meaningful patient-to-provider interaction," says Ream. "Ensuring that patients receive the time and attention they need, without technology interruptions during their clinic visits, is extremely important for improving patient satisfaction. With Hands Free Authentication, prescribers no longer have to pay attention to multiple screens or manually enter multiple passcodes. Instead, prescribers remain patient-based while enjoying the more efficient, technology-enabled workflows."

Lessons Learned

- Collaborate with your EHR and Dual-Factor Authentication solutions
- Deliver a simple well defined implementation strategy
- Include your Informatic's team members for pilot stage and/or providers for feedback
- Offers a hands-free solution with the product giving providers more face time with patients
- Delivered solid robust redundant system architecture