CISCO SECURE | DUO

Epic Hyperdrive

Epic is a leading healthcare software provider for systems that manage electronic healthcare records (EHR). Hyperdrive is Epic's new flagship Electronic Prescriptions for Controlled Substances (ECPS) healthcare management software delivered through modern web protocols. Duo's integration with Epic Hyperdrive helps prevent unauthorized users from accessing patient data.

THE CHALLENGE:

Safeguarding Healthcare Organizations from Breaches of Protected Health Information (PHI)

In 2022, 66% of healthcare organizations were targets of ransomware attacks, up from 34% in 2020. Almost all of these attacks targeted patients' protected health information (PHI) such as medical records and social security numbers.

Typically, attackers phish to steal credentials and ultimately gain access to patient data. With the patient data on hand, attackers commit identity fraud, access medical care in the patient's name, or send patients spam emails.

THE SOLUTION:

Duo's Trusted Access

Duo's Trusted Access solution benefits healthcare organizations in a couple ways:

**1. Helps Prevent Unauthorized Access to Patient Data**

Multi-Factor Authentication (MFA) is essential to guarding access to patient records by ensuring only authorized personnel gain access. Duo's cloud-based MFA solution integrates out-of-the-box with Epic Hyperdrive, allowing clinicians to authenticate with Duo before they access patient records or sign e-prescriptions.

2. Helps Meet EPCS Compliance Requirements

Duo's MFA solution can help healthcare organizations meet EPCS (Electronic Prescription for Controlled Substance) compliance by providing clinicians a variety of authentication methods such as Duo Push, mobile one-time passcodes (OTP), hard token OTPs, and YubiKeys.

The Duo + Epic MFA Workflow

0 — The admin downloads a key from Duo Admin Panel and uploads it to Epic, which uses the key to establish trust during authentication.

1 — Client submits username & password to Epic.

2 — Epic validates the credentials then sends a response to let the Client know.

3 — Client presents user with MFA options; the user selects one and the Client sends a request to Duo for MFA. For Push authentications, the flow is:

a — (click) Duo sends Push authentication request to the user's mobile phone.

b — (click) User confirms Duo Push on their Mobile Phone.

4 — Duo validates and returns a SAML assertion.

5 — Client forwards the SAML assertion to Epic for validation.

6 — Epic validates the SAML assertion and grants access.
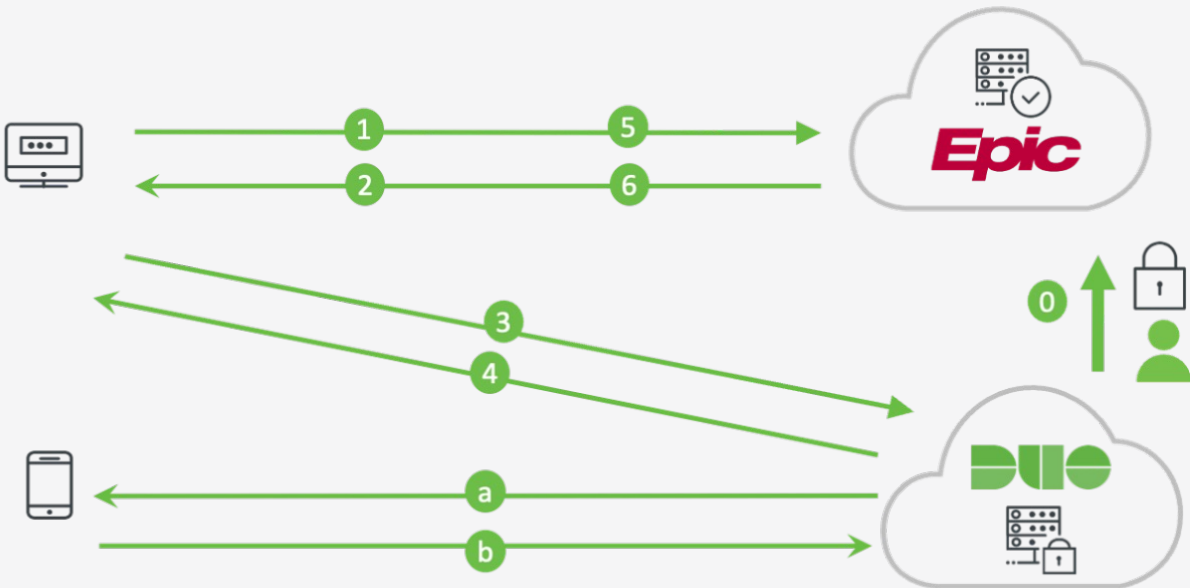
Learn how Duo can help you with Epic at **duo.com**

> "Duo integrates with Epic, which means we were able to be an early adopter of EPCS functionality in Epic, with 1000+ providers currently enrolled."

Security Manager, Large Enterprise Healthcare Company

Take Duo for a spin

with your **free 30-day trial** and learn why thousands of customers have made us the most loved company in security.

Start at **signup.duo.com.**

DUO

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 40,000 customers globally, including Yelp, Box, Generali, La-Z-Boy, Eastern Michigan University, Sonic Automotive and more.

Try it for free at **duo.com**.

CISCO SECURE

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at **cisco.com/go/secure**.

866.760.4247

duo.com

CISCO The bridge to possible