FlexPod®

FIPS 140-2 security-compliant FlexPod solution for healthcare

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) 140-2 is a U.S. government standard that sets security requirements for cryptographic modules in hardware, software, and firmware that protect sensitive information. Compliance with the standard is mandated for use by U.S. government agencies, and it is also often used in such regulated industries as financial services and healthcare.

What do providers get out of compliance?

Eligible providers and hospitals are required to use a FIPS 140-2 (level 1) compliant HIT for receiving Medicare and Medicaid incentives and for avoiding reimbursement penalties from the Center for Medicare and Medicaid (CMS). FIPS 140-2 certified encryption algorithms qualify as technical safeguards that are required as per the Security Rule of the Health Information Portability and Accountability Act (HIPAA).

Providers are not just responsible for their networks, but also for their vendor networks. Examples of hospital business associates and vendor networks include:

• Life science labs

• Research labs

• Rehabilitation facilities

• Community hospitals and clinics

CISCO NetApp

The following graphic is a small example of the possible associated vendor networks for a hospital system:
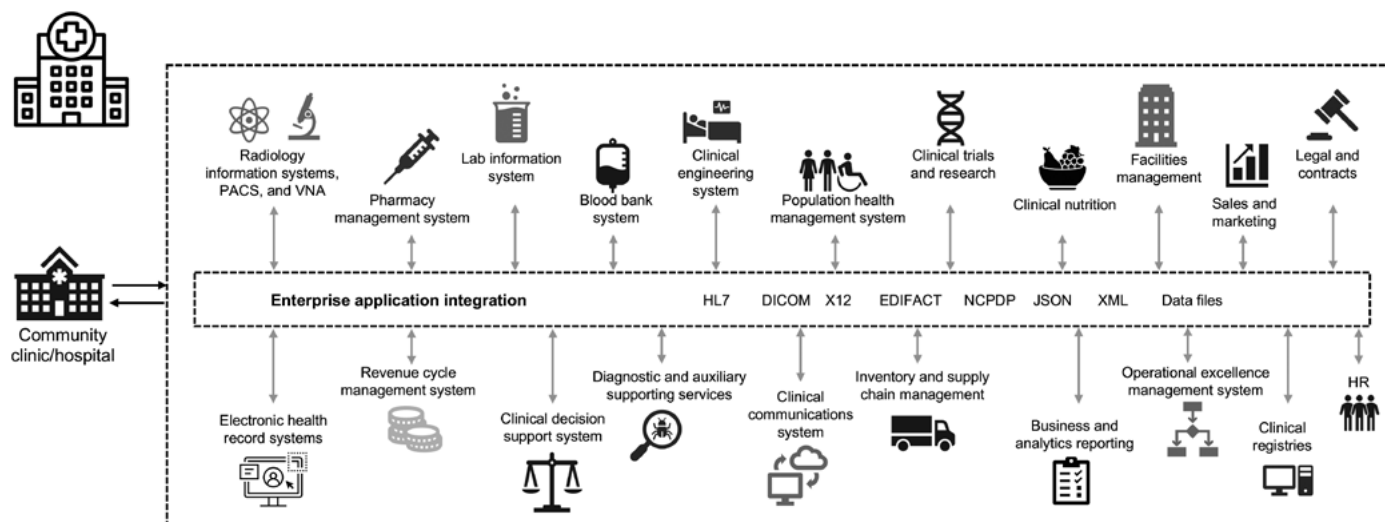
Why FlexPod with FIPS 140-2?

- Some Cisco UCS servers are designated FIPS 140-2 compliant.

- Cisco UCS Manager is also FIPS 140-2 compliant.

- Cisco MDS 9000 series switches are FIPS 140-2 compliant.

- Cisco Nexus 9000 series switches are also FIPS 140-2 compliant.

- NetApp® ONTAP® software is FIPS 140-2 compliant for data-in-transit and data at rest.

- NetApp can also provide self-encrypting drives (SEDs) that are FIPS 140-2 validated.

For more information, view the entire document:
TR-4892: FIPS 140-2 security-compliant FlexPod solution for Healthcare.