Kodiak Systems

Six healthcare IT buzzwords you can beat

It's not your fault—jargon can be intimidating. But you don't need to let it win.

Outcome-based healthcare IT can help you focus your organization on its core mission and competencies. But that's hard to do if you get mired in the complexities of IT production. How can you optimize your business and improve patient outcomes when just keeping up with IT terminology makes your head spin?

The IT department wants to help, but sometimes they can lose you in the minutiae—ask a simple question about file transfers, and you wind up feeling like you're listening to a couple of baseball nuts debate box scores.

Get up to speed

Buzzwords and jargon may create a useful shorthand for insiders, but they can make the rest of us feel out of the loop. Here are brief definitions of six essential but often poorly understood components of modern healthcare IT. Use this glossary to have more productive conversations with your IT partners, understand your options more clearly, and make decisions with more confidence.

1. Endpoint management

The discipline of managing groups of computers and other devices running multiple desktop and mobile operating systems. Endpoint management is the continuous and ongoing practice whereby network administrators manage and integrate software distribution and updates, access control, and antivirus protection. Businesses use endpoint management to cope with increasing complexity, reduce overall IT costs, streamline system management, and manage risk.

2. Enterprise mobility management (EMM)

A pillar of digital transformation. In today's healthcare IT context, businesses must empower workers with uninterrupted access to the tools they need. EMM refers to suites of software, services, and processes that organizations use to integrate mobile devices, wireless networks, and other mobile computing resources with their existing IT environments, work processes, and business objectives—in a way that minimizes the need for continuous IT administration.

Popular vendor: *Microsoft*

3. Application whitelisting

The practice of preventing users from introducing unauthorized programs or applications into a network environment, as well as the technology used to do so. The objective is to safeguard the network from malware and other viruses that may infect it through an unapproved application. When any program attempts to execute within the network, an application whitelisting solution checks it automatically against an approved list, then blocks the program if it's not included. In modern healthcare IT, application whitelisting is a best practice for security.

Popular vendors: *Carbon Black, Symantec, McAfee (Intel Security)*

4. Imaging

Used by IT administrators for OS deployment, configuration, PC migration, and software deployment across hardware platforms and operating environments. You can use imaging to install or test operating systems and other programs quickly without risk of corrupting other network assets. It increases IT efficiency, lowers costs, and reduces downtime by automating deployment and configuration processes. Imaging is critically important and valuable in fast-growing, dynamic IT production environments.

Popular vendors: *Altiris, Symantec*

5. Multifactor authentication (MFA)

Requires users to verify their identities using more than one set of credentials before they can sign in to a network, database, application, or device. MFA credentials typically include a password, a security token, and/or some kind of biometric verification such as a fingerprint, a retinal scan, voice waveform recognition, or facial recognition. It makes unauthorized access more difficult and helps mitigate the vulnerability of traditional password databases and the threat of brute force attacks. MFA has become a security best practice in healthcare IT, often per compliance requirements.

6. Web filtering

Used to screen incoming web pages and determine whether they should be displayed. A web filter checks content against the programmed rules that are updated regularly to match the changing threat landscape. It allows an enterprise to block objectionable content and to screen web content for viruses and spyware. Web filtering is considered part of a complete risk management system—often per compliance requirements—and a security best practice in healthcare IT.

Popular vendors: *Forcepoint, Cisco, Barracuda Networks*