THE DOCUMENT COMPANY
XEROX

Market Brief

Security and the Healthcare Industry

Meeting healthcare regulations for security & privacy

The new standard

HIPAA, the Health Insurance Portability and Accountability Act, requires that all healthcare organizations apply uniform data management practices across their enterprises. At the heart of HIPAA is the vigorous protection of patient information and patient privacy.

Distribution of patient information to both the clinical community and the patient under HIPAA requires an audit trail that documents who has viewed patient data, when it was viewed, and that the person viewing the data has the proper authorization and consent. This virtually forces electronic distribution of patient information. As a result, an extra burden falls on the healthcare industry to ensure that their IT systems and devices also provide the necessary level of security.

Common Criteria Certification

Common Criteria Certification has emerged as a standard by which all industries can evaluate the security of their information systems and devices. This rigorous process provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. Common Criteria Certification is required for devices used by the federal government for national security to ensure the integrity of the government's most sensitive and critical data. Other industries, including healthcare, can benefit from the government's initiative by choosing devices that have achieved Common Certification Criteria.

Front and center with security

At Xerox, information security issues have always been front and center. As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure. And now, with Common Criteria Certification, Xerox customers in the healthcare industry have an extra measure of confidence that their information is absolutely safe and that they are exercising the due diligence required by HIPAA.

The Challenge:

The Health Insurance Portability and Accountability Act (HIPAA) requires that healthcare organizations exercise "due diligence" in an effort to ensure the security and privacy of patient information. Given the subjective nature of HIPAA, healthcare organizations may find it difficult to determine if they are meeting the standard.

The Solution:

By adopting standards that federal government agencies must meet for information security – arguably the toughest standards in existence today – healthcare organizations can be confident that they are meeting the security and privacy mandate set down by HIPAA. Office devices that have received Common Criteria Certification for use in national security by the federal government can provide the highest level of security available to the healthcare industry.

The Xerox Advantage:

In addition to delivering exceptionally well-architected and highly productive devices into the office environment, Xerox has received Common Criteria Certification for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55. As part of the certification process, the security of the embedded fax function of these devices was also validated. *No other multifunction device manufacturer has obtained third-party assurance that fax and network lines are separated.*

THE DOCUMENT COMPANY
XEROX

Call today. For more information about Xerox Common Criteria Certification, security initiatives, or office solutions, call **1-800-ASK-XEROX** or visit us at **www.xerox.com/office.**

Commitment to Security and the Common Criteria

Xerox offers a variety of solutions that maximize productivity and security.

Embedded Fax – Prevents unauthorized access to the device via the fax subsystem because it is internally separated from network functions. *No other multifunction device manufacturer has obtained third party assurance that fax and network lines are separated.*

Image Overwrite – Electronically eradicates data processed to the hard disk during print, scan, or e-mail operations by repeatedly overwriting the data.

Device Access Password Protection – Administrative set-up screens and remote network settings cannot be viewed or altered without a personal identification number (PIN). This controls access to all device functions.

Secure Print – Holds jobs until the job owner enters a PIN to release them for printing to prevent unauthorized viewing.

Removable Disk Drive Accessory – The removable hard drive may be taken out and stored for maximum security.

Network Authentication – Restricts access to scan, e-mail, and network fax features by validating network user names and passwords prior to use of these features.

IP Address Restriction – Administrative set-up screens allow access to be restricted for specific IP addresses to control communications with specific network clients.

Achieving Common Criteria Certification

Common Criteria Certification for the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 was completed by Computer Science Corporation, an accredited Common Criteria Testing Laboratory. The security functions certified include:

Image Overwrite – During normal operation, a multifunction device temporarily stores image data on the hard drive. The image overwrite function eradicates customer data by repeatedly overwriting the disk surface with specific patterns of data. At the end of the procedure it reads a portion of the overwritten area – typically 10% – to make sure that only the last pattern written can be read. This ensures that no normal read process can discover the original customer data. The overwrite mechanism complies with the 3-pass process specified in the U.S. Department of Defense Directive 5200.28-M. The image overwrite function eradicates data once a job is completed or when invoked at any time by the system administrator.

Authentication and Security Management – Only system administrators authenticated via a personal identification number can access the security settings of the device. Network authentication further restricts access to scan, e-mail, and fax features by validating network user names and passwords prior to the use of these features.

Data Flow Security – The secure embedded fax ensures that malicious users cannot access network resources from the telephone line via the device's fax modem because the fax subsystem is internally separated from network functions. Additionally, faxes can be automatically routed to a password protected fax mailbox or stored at the device until an authorized user releases them for printing.

XEROX
Worldwide Partner