



# HIPAA and imageWARE

## Protecting Patient Health Information

### About HIPAA

The 1996 Health Insurance Portability and Accountability Act (HIPAA) mandated that the Department of Health and Human Services, known as DHHS, develop a set of high-level information security and privacy standards. The new standards have become federal regulations and HIPAA requires organizations to design and enforce compliance policies.

### Compliance

Organizations become HIPAA-compliant by enforcing policies and procedures that safeguard the privacy and security of patient health information and records. Technology can help organizations comply with the HIPAA standards. Here we identify imageWARE Document Manager functions that can help enforce HIPAA's Privacy and Security requirements.

### Privacy Rule

This rule requires that all reasonable measures are taken to ensure the confidentiality, integrity, and availability of individually identifiable patient health information. The Privacy Rule became effective on April 14, 2001.

### Security Rule

This rule proposes standards to provide a uniform level of protection for all health information that is stored or transmitted electronically.

<b>HIPAA Requirement</b>	<b>imageWARE Functionality</b>
<b>Confidentiality</b>	Sending information by e-mail rather than fax ensures that it is delivered to a private e-mail account rather than a public fax machine. Faxes can be automatically forwarded from compatible imageRUNNER devices to Document Manager folders securely.
<b>Disclosure Auditing</b>	Document Manager maintains a detailed audit trail of user actions and document operations. Whenever a document is distributed from an imageRUNNER device, a copy of the sent document can be archived in the Document Manager. Document Manager is integrated with Lotus Notes-based systems, allowing you to save a copy of all outbound messages with external addresses on the Notes server.
<b>Minimum Disclosure</b>	Binders can be created containing just those documents or pages of documents that will need to be distributed to external parties. Using drag-and-drop, binders can be faxed or e-mailed, sending just those pages in the binder. Also, annotations tools allow you to cover sensitive information before delivering it to an external party.
<b>Encryption</b>	Optional encryption of Document Manager passwords and volumes is available using government-approved encryption methods.
<b>Disaster Recovery</b>	Document Manager cabinets are simple to back up and send offsite for access in case a disaster occurs.
<b>Information Availability</b>	Document Manager makes documents available via a Windows-base interface or over a secure Internet connection. Information can be distributed using drag and drop by fax, email, and print.
<b>User Authorization</b>	User access can be authenticated against a Windows domain, Lotus Domino server, or the Document Manager server for maximum security and consistency across the network. This ensures that only authorized individuals can view documents.

**You can find additional information about Canon imageWARE products by visiting the imageWARE Web site at [www.imageware.com](http://www.imageware.com).**