



**Med Docs**<sup>TM</sup>  
Patient Records Management System

---



**MedDocs**<sup>TM</sup>  
**Electronic Patient Records  
Management System**

**Product Information**



Ask about MedDocs<sup>TM</sup> Key a secure zero footprint portable  
Patient Personal Medical Records  
Management application



MedDocs™ (MD), is a feature rich Electronic Patient Records Management System designed by Integrated Digital Systems/ScanAmerica, Inc. with over 15 years of Records and Document Management experience and over 5 years experience in medical and patient related file conversion, hosting services and HIPAA application. MD is primarily designed to provide Healthcare Providers a way to better or more cost effectively manage patient files, forms, X-rays, film and other related medical documents and meet HIPAA requirements. The most unique features of MD which also sets it apart from other Electronic Record Management System applications are:

- HIPAA compliancy,
- HL7 Reporting Interface (optional)
- Medical Forms Manager,
- Patient MedKey Interface
- Patient Appointment Scheduling
- Medical Record Printing and Fax (with permissions)
- Remote Coding Capabilities (optional)
- Wireless Tablet PC Ready with XP Tablet Journal feature
- Barcode Capture and Patient Information label printing ,
- Barcode Coversheet Generator for Patient Charts Capture
- Log and Email Feature
- DICOM Image Viewer for X-ray and Medical Film display
- Batch Scanning and Indexing
- Transaction Logging and Activity Logging
- Physician defined Patient File and Document Index Values
- Archive Offline Feature
- Access Database upgrade to MS SQL 6.5 and later with SQL Wizard.



# Med Docs™

Patient Records Management System

---

- Smartcard, USB Token and RFID Proximity Security Capability

These features represent the ultimate in Patient record applications and their use. Other standard MD features include:

- New active Search and Select GUI
- Secure Administration Module
- New File and Document Selection feature
- Add new files from Scan enable copiers and printers
- Rules and Roles Workflow ( Practice Process ) interface upgrade (optional)
- Email and attachment file storage capability
- Image Thumbnails (TIF images only)
- Email File Routing
- Bates Numbering feature ( Unique#, date and time )
- Secure Internet Access via MedLink™
- Batch Document Processing
- Secure Hosting Services (optional)
- Enhanced Export to Media feature with MedDocs Viewer
- New Auto Archive and Retrieve feature
- Local Secure login or Windows Authentication Login using Active Directory
- Microsoft Office 2003 and 2007 compliant
- SQL Database wizard
- Microsoft SQL Server Create Tables Utility.
- Administration Module with features to create users, groups, set group permissions, use of Active Directory, implements Access Logging, Folder Retention and the export of each category into MS Excel.
- Automatic log-off from the application after 15 minutes or immediate with



# Med Docs™

Patient Records Management System

---

- Proximity feature.
- Store and Open all PDF formats, all Microsoft Office formats, most graphic file formats, X-rays, Film and many more
  - Storage of transcribed sound files, video, and executable files with a link to the native application
  - Open links in Office documents and emails in documents
  - Capture Group IV single and multi-page Tiff document images from a MFP or any TWAIN compliant scanner
  - Ability to quickly apply file and document index data
  - User ability to add and delete required folder and document index fields to insure proper document identification
  - Manage documents in a stand-alone or shared networked environment
  - Import pictures, PDF documents, MSOffice documents, Radiology Film Images, tiff documents, email, rtf files, color graphics and digital photography in Patient file
  - Ability to search for documents and folders using index data
  - Ability to Print individual documents or complete files
  - Ability to Import Group IV – VII TIF image batches and apply index data
  - Easy export of documents, folders and metadata to Xerox DocuShare, EdgeVault, Sharepoint, and Edge Workflow™ seamlessly
  - Rotate and zoom in on clear, sharp images
  - Export documents to popular OCR/ICR software
  - Store and retrieve documents locally or on a Network Dir., NAS, SAN, or Optical Media
  - Redact scanned TIFF documents containing sensitive data
  - Highlight, outline, annotate, rubber stamp, add sticky notes, and underline text in



unlimited colors in scanned TIFF documents.

MD can collectively store over 200 document types including email attachments, entire Microsoft Office 2003 and 2007 Suite, Standard Medical Forms Selection and Management, Medical film images in color, PACS Images, and digital photographs. Each Patient Record can have up to 14 metadata fields (Patient Information) for each Patient file and 15 individual document indices (Define electronic document/image type and content ). The following are examples of documents types /image index references that a document index might contain :

- **Demographic Information:** A summary of the patient history, contact information and personnel information for providing medical services.
- **Progress Notes:** This feature keeps track of progress notes taken by Physician/Doctor during each appointment or contact with with the patient.
- **Lab Reports:** This feature enables to store the type of tests taken on the patient and also logs in the results of the same.
- **Radiology and X-Ray Reports:** This feature helps to log the information about the patient X-Ray Reports and EKG Reports. MedDocs™ will accept radiology images captured from VIDAR medical film scanners and other PACS systems.
- **Miscellaneous Supporting Documentation:** MD stores information about physical examinations conducted on the patient and other information like drugs which are allergic to the patient, any hereditary disorders that the patient might have inherited and other important supporting information.
- **Consultation and Hospital Reports:** This features logs in Hospital Reports; which for example may have been recorded when patient is being discharged from hospital after an operation.



# Med Docs™

Patient Records Management System

---

MD provides for the selection of blank medical forms, completion of the forms and placement in the patients file. Standard forms can be easily added through the Forms Administration module and selected under add document feature. Documents can be gathered through the add document function from sources like Fujitsu or other TWAIN compliant Scanners, Multifunctional Devices (scan, print, copy products), Windows Explorer ( drop and drag ), Forms Templates , Email ( with attachments ) , and Group IV TIFF image batches.

With the growing demand for effective way of organizing and sharing a patient's medical documents it is imperative to digitize these records for easy access. MD was designed to be an easy to use, flexible, open, and customizable application to handle the demands of hospitals, physician offices and primary healthcare centers today. With a Personal Computer, and or a Desktop Scanner or scan enabled copier a medical assistant is fully equipped to manage a wide range of medical documents and meet the demands of the new eHealthcare initiative.

To meet the demands of today's new regulations and HIPAA requirements MD features provide :

- front-end paper batch capture/scanning,
- barcode reading and printing,
- log-in ID and password,
- activity tracking and logging,
- Active Directory interface,
- 15 minute auto log-out feature and much more.
- Patients or requesting Physicians can be provided copies of individual healthcare records through email with logging or the export feature of MD.



# Med Docs™

Patient Records Management System

---

- An individual patient file can be exported to the CD Directory feature in Windows XP and placed on CD-ROM or DVD Media with a MD Auto-run Viewer. Or placed on a MedKey portable device.
- Secure MedLink™ Server and thin client access anywhere anytime.

MD records can be backed-up locally or stored on the HealthDocs™ secure web repository for a low monthly fee.

MD records can be automatically archived, searched and retrieved using the built in records archiving and search features. Archiving provides a means to store and protect patient records according to medical record retention guidelines.

The standard out of the box version of MD has a Microsoft SQL Express database integrated into the product so it is ready to run on Physicians Office or Clinic workstations running Vista, Windows 7, Windows XP and Microsoft Office 2003 or 2007. The information captured and stored in the database provided with the product can also be easily migrated to Microsoft SQL ODBC database structures to meet the demands of secure and robust databases as well as growth.

## **MedLink™ Sever**

MedLink™ is a secure web based interface integrated with MedDocs™. MedLink™ provides a permissions controlled secure view of Patient records over the Internet.

MedLink™ is a secure web browser accessible server application that is linked directly with customers' MedDocs™ thick Client Application that grants users easy and secure access to add, store, retrieve, email and share documents stored in MedDocs™ over the Internet, Intranet, Wide Area Networks, VPN and other secure connections.

The MedLink™ product provides MedDocs™users secure remote access to their records. The product may reside on your IIS server and your database and the Image Directory can



reside on the same server or a separate server. Administrators will only have to update information once for each different client application configuration of MedDocs™. Access is protected using an ID and Password in Secure Admin, or Active Directory. MedLink provides for SSL and HTTPS encrypted access. RSA or USB Token security is available for dual authentication.

MedLink™ goes hand-in-hand with our MedDocs™ Client/Server application. Since the thick and thin clients share the same database and image directory, all files and folders created or updated in one will be available in the other. MedLink™ logs all access and changes by user access ID and password.

#### **Features in MedLink™:**

- File Ownership
- Microsoft ® Office 2003 & 2007 compliant
- Windows Authentication Login using Active Directory
- Store and Open in MedLink™ all PDF formats, all Microsoft Office formats, most graphic file formats, Visio and many more
- Storage of Sound, Video, and executable files with a link to the native application
- Open links in Microsoft® Office documents and emails in documents
- Ability to quickly apply file and document index data
- Import pictures, PDF documents, tiff documents, email rtf files, graphics in file folders
- Ability to search for documents and folders using index data
- Ability to email and export documents with automatic conversion
- Ability to Print images or complete folders with permissions
- Ability to share MedDocs™ access over a network with MedLink™
- Store and retrieve documents from the secure Server
- Allows users to Add, Delete, Edit, View, and View Properties of each folder.
- Documents can be Added, Deleted, and Emailed through the MedLink™ client based permissions.
- Provides secure access to your records from anywhere by anyone with permissions



based on a valid username and password stored within the MedLink™ Server or Active Directory.

- Administrators can create individual user accounts or group accounts, as well as Add, Edit, and Delete folder and document fields from the Field Manager.
- Folders and documents are protected by permissions. The owner of a folder or document can give individual or group permissions that allow only those specified users to view or edit the document.

### Add on Modules

The development of MD in Microsoft's .NET Development platform with installing features like OLE, ODMA, ODBC, and Open Architecture capabilities, makes MD an open, but secure product that comes with features that are fully integrated with other products such as :

- Microsoft Sharepoint
- Microsoft SQL versions 6.5 and up
- Most Multifunction Devices
- Open Architecture Third Party Medical Accounting Systems
- Edge Workflow™
- Microsoft Office 2003 & 2007

### HIPAA Compliance Features:

\*At least one of the following must be implemented: **Red text** =Minimum **Blue text** = means exceeds minimum

HIPAA Requirement	Requirement Description	MedDocs™ Compliance Feature
Access		



# Med Docs™

Patient Records Management System

HIPAA Requirement	Requirement Description	MedDocs™ Compliance Feature
	<p><b>*Role-based access</b> -- is an alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.</p>	<p>Through the Administration Module role-based access can be given by creating and assigning groups and their privileges. The available privileges to set for each group are: Administration, Delete, Scan, DocuShare, SharePoint, Add, Edit, Index, EdgeVault, Workflow, Archive, Email, Export, iManage. You can also set which members can be available to each group when creating new groups.</p> <p>Active Directory is an essential component of the MedDocs™ architecture which presents organizations with a directory service designed for importing the Windows 2008, Windows 2003, and Windows NT 4 operating systems users across each domain. This feature improves manageability by centrally managing Windows users of each domain through a single consistent management interface, reducing redundancy and maintenance costs.</p>
	<p><b>Access</b> - refers to a security mechanism users of a system access based upon the user.</p>	<p>User-based access is the default access control mechanism. Users are assigned a user name and password by the administrator. User accounts can be assigned to a group and their account can also be set as active or inactive status. The Windows 2000, Windows 2003, and Windows NT 4 operating systems use Access Control Lists (ACLs) to protect files, applications, and other resources from unauthorized use. ACLs can be used to grant permission at either the user account or group level. Microsoft's information storage technologies (Microsoft SQL Server and Web Store) also provide the ability to assign permission at the user or group level.</p> <p>Active Directory is an essential component of the MedDocs™ architecture which presents organizations with a directory service designed for importing the Windows 2000, Windows 2003, and Windows NT 4 operating systems users across each domain. This feature improves manageability by centrally managing Windows users of each domain through a single consistent management interface, reducing redundancy and maintenance costs.</p>



# Med Docs™

Patient Records Management System

HIPAA Requirement	Requirement Description	MedDocs™ Compliance Feature	
	<p><b>Audit Controls</b> - Log system activities into a common log file, including record view, add, update, and delete activities.</p>	<p>Access Logging options are defaulted to on. An administrator must use the Administration Module to turn off logging options</p> <p>Access Logging options can keep track of when a record was viewed, added, updated, and/or deleted. The following data is logged for each function that is turned on with in the Access Logging section of the Administration Module: History ID, User ID, Station ID, Function Performed, folders Main ID, Documents ID, and a Time Stamp of when each function was performed.</p> <p>Available Access Logging options: Administration, Delete, DocuShare, SharePoint, Add, Update, EdgeVault, Workflow, Archive, Log In/Out, iManage.</p> <p>Added logging options to MedDocs Secure are: EdgeGuard</p>	
<b>Data Authentication</b>			
	<p><b>Automatic Log-off</b> - a security procedure that causes an electronic session to terminate after a predetermined time of inactivity, such as 15 minutes.</p>	<p>Traditional applications can utilize functionality of the Win32 API to logoff the system. Built into our product is an automatic log-off mechanism that automatically logs the user out of our application after the mouse has been idle for 15 minutes. In addition RFID Proximity Readers can be installed to provide immediate log-off when a user steps away from the PC.</p>	
	<p><b>Unique User ID</b> - a combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity.</p>	<p>Each individual user is assigned a user ID based on the order in which the users were created.</p>	
	<p><b>*Biometric</b> - an identification system that identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).</p>	<p><b>Biometrics can be used on a PC level using client/server authentication.</b></p>	
	<p><b>*Password</b> - refers to confidential authentication information composed of a string of characters.</p>	<p>Passwords are assigned by the administrator and they are encrypted using a sting of characters.</p> <p>Active Directory is an essential component of the MedDocs™ architecture which presents organizations with a directory service designed for importing the Windows 2000, Windows 2003, and Windows NT 4 operating systems users across each domain. This feature improves manageability by centrally managing Windows users of each domain through a single consistent management interface, reducing redundancy and maintenance costs.</p>	
	<p><b>*Token</b> - refers to a physical item necessary for user identification when used in the context of authentication. For example, an electronic device that can be inserted in a door or a computer system to obtain access.</p>	<p><b>Windows 2000 and Windows 2003 operating systems supports authentication via a Smart Card, Proximity RFID, or RSA USB Token or at a client level on Windows XP.</b></p>	



# MedDocs™

Patient Records Management System

HIPAA Requirement	Requirement Description	MedDocs™ Compliance Feature
<b>Transmission Security</b>		
	<p><b>Integrity Controls</b> - ensures data integrity by providing detection of unauthorized modification of data. Security mechanism employed to ensure the validity of the information being electronically transmitted or stored. Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.</p>	<p>MedDocs™ with EdgeGuard™ uses PKI technology to ensure the integrity of transmitted documents by using digital certificates to validate a user's identity, ensure that the document has not been changed or corrupted in transit, as well as protecting the information from interceptions during transmit.</p>
	<p><b>*Access controls</b> - refers to a method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, and classification.</p>	<p>Active Directory is an essential component of the MedDocs™ architecture which presents organizations with a directory service designed for importing the Windows 2000, Windows 2003, and Windows NT 4 operating systems users across each domain. This feature improves manageability by centrally managing Windows users of each domain through a single consistent management interface, reducing redundancy and maintenance costs. User-based access is the default access control mechanism. Users are assigned a user name and password by the administrator. User accounts can be assigned to a group and their account can also be set as active or inactive status.</p>
	<p><b>*Encryption</b> - refers to transforming confidential plaintext into ciphertext to protect it. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.</p>	<p>Transmitted data can be encrypted using a variety of public key or private key encryption mechanisms. MedDocs™ with EdgeGuard™ uses PKI which allows users to send and receive information securely (using encryption) and be sure that the person sending the information is who they say they are by their digital signature.</p>
<b>Electronic Signature</b>		
<p>Features within MedDocs™ are compliant with following US and international legislations and complies with Industry</p>	<p><b>Message Integrity</b> - the assurance of unaltered transmission and receipt of a message from the sender to the intended recipient.</p>	<p>In using MedDocs™ with EdgeGuard™ documents signed with a digital ID are verifiable in the follow ways: By the use of timestamps and by the inclusion of a hash, or fingerprint, of the document. MedDocs™ with Edge Guard™ uses PKI technology to ensure the integrity of transmitted documents by using digital certificates to validate a user's identity, ensure that the document has not been changed or corrupted in transit, as well as protecting the information from interceptions during transmit.</p>



# MedDocs™

Patient Records Management System

HIPAA Requirement	Requirement Description	MedDocs™ Compliance Feature
Standards currently in operation in worldwide.	<p><b>Non-repudiation</b> - strong and substantial evidence of the identity of the signer of a message, and of message integrity, sufficient to prevent a party from successfully denying the origin, submission, or delivery of the message and the integrity of its contents</p>	<p>MedDocs™ with EdgeGuard™ uses PKI technology to ensure the integrity of transmitted documents by using digital certificates to validate a user's identity, ensure that the document has not been changed or corrupted in transit, as well as protecting the information from interceptions during transmit. By encrypting the document using the digital ID, the privacy of the document's contents is assured. If the document is encrypted using the public key, only the person with the corresponding private key may decrypt it. By applying a timestamp to a signature, it is then possible to prevent a person from denying having signed a document at a particular time. This also offers a way of preventing previously used signatures, from being reused.</p>
	<p><b>User Authentication</b> - the provision of assurance of the claimed identity of an entity</p>	<p>If the document is encrypted using the public key, only the person with the corresponding private key may decrypt it. If the other person does not have the corresponding key the document cannot be decrypted or viewed.</p>
	<p><b>*Ability to add attributes</b> - one possible capability of a digital signature technology; for example, the ability to add a time stamp as part of a digital signature</p>	<p>In using the wizards that are available in MedDocs™ with EdgeGuard™ it allows the ability to add Time Stamping, Document Approval, Multiple Signatures, and Legal Ceremony Testimonials. The date and time are included in the signature, so they cannot be gainsaid.</p>
	<p><b>*Continuity of signature capability</b> - the concept that the public verification of a signature must not compromise the ability of the signer to apply additional secure signatures at a later date</p>	<p>MedDocs™ with Edge Guard™ allows you to apply your digital signature to a previously digitally signed document you have received. This feature is useful if two or more people are required to digitally sign the document, and works rather like several people applying physical signatures to a legal document.</p>
	<p><b>*Counter Signatures</b> - The capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that has already been signed by another party</p>	<p>MedDocs™ with Edge Guard™ allows you to apply your digital signature to a previously digitally signed document you have received. This feature is useful if two or more people are required to digitally sign the document, and works rather like several people applying physical signatures to a legal document.</p>
	<p><b>*Independent verifiability</b> - the capability to verify the signature without the cooperation of the signer</p>	<p>In order to verify the signature without the cooperation of the signer the recipient has to have the corresponding private key to do so.</p>
	<p><b>*Interoperability</b> - the applications used on either side of a communication, between trading partners and/or between internal components of an entity, are able to read and correctly interpret the information communicated from one to the other</p>	<p>EdgeGuard Reader™ is needed to view encrypted and signed emails and documents if the document was encrypted using MedDocs™</p>



### **Service and Support:**

Service and support is provided thru an 800#, and Online HelpDesk. IDS provides technical support services not only for MedDoc's customers but for Microsoft Products and a wide range of other third party hardware and software products.

For more information about this or any of the complete line of Edge and Microsoft products contact Integrated Digital Systems @ [Sales@idsscan.com](mailto:Sales@idsscan.com) , call 1-800-283-0999 or Visit [www.idss.net](http://www.idss.net).