KONICA MINOLTA

WHITEPAPER

HIPAA AND HITECH COMPLIANCE

SAFEGUARDING YOUR CONFIDENTIAL PATIENT INFORMATION

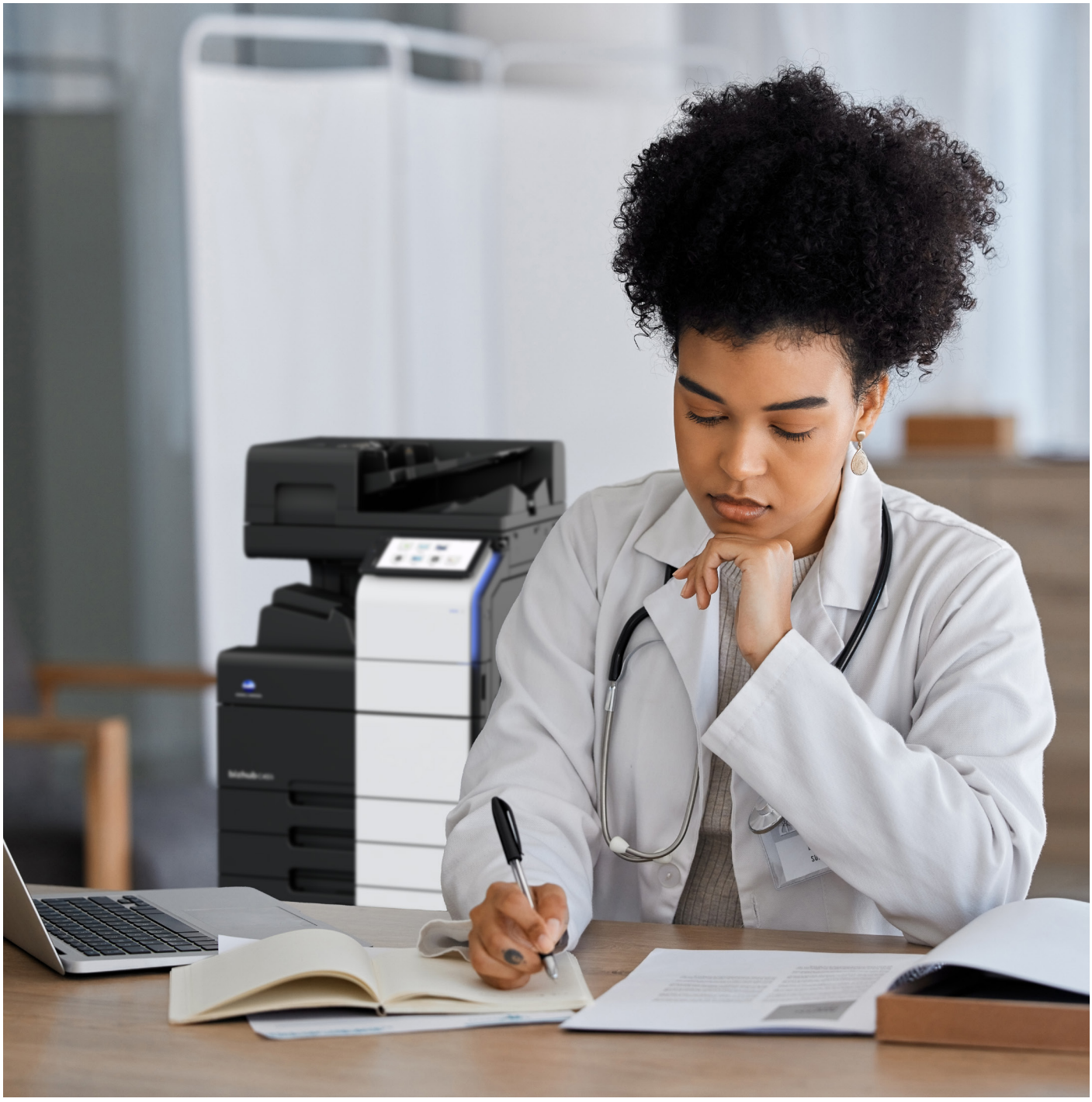


TABLE OF CONTENTS

NOTE: Some of the specific security features and options described in this report may only apply to specific Konica Minolta bizhub models. It is best to refer to the documenta- tion that is provided with every Konica Minolta bizhub MFP to verify exactly which security features are included with a specific product. It is also important to note that a specific machine may require an upgrade to achieve and/or enable some of the features discussed in this report. Please refer to your service representative for further information.

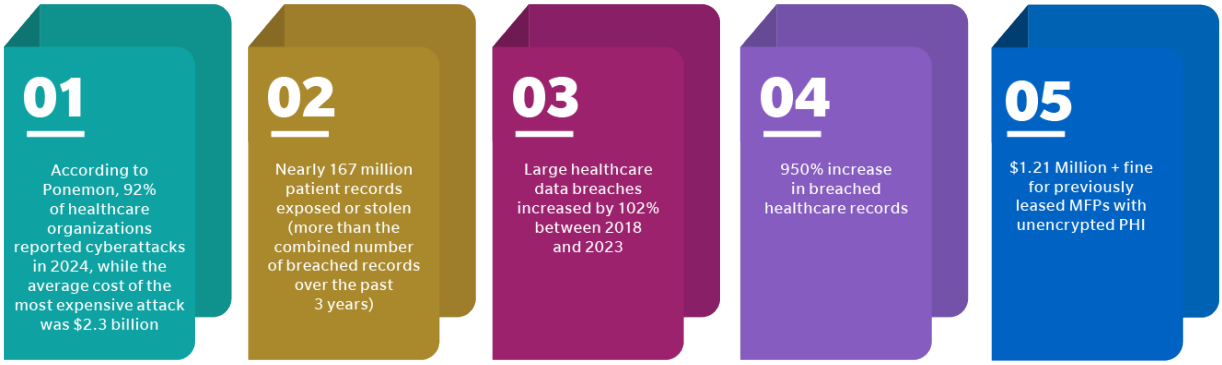
INTRODUCTION

The complexity of healthcare in the United States has soared, making everything from reimbursement to regulatory compliance ever more challenging for providers, payers and patients. Healthcare expenditures in the United States have grown at an astounding rate, and currently comprise 18% of the US Gross Domestic Product (GDP), equatingto $3.8 trillion. Industries with economic implications this significant require extensive fiduciary responsibility to ensure proper and ethical management over the resources, data, processes, and services that make up that ecosystem. And at a time when large data breaches are almost a weekly occurrence across all industries, the confidentiality and protection of patient data is perhaps one of the greatest challenges faced by the medical community. Recent breaches of Protected Health Information (PHI) have resulted in civil penalties and fines reaching into the millions of dollars, including a health plan fined $1.2 million for PHI found on unprotected and unencrypted MFP hard drives.

Information security has become critically important as various organizations and businesses use their electronic systems to comply with government regulations. Recent laws and regulations include:

- Medicare and Medicaid Promoting Interoperability Program
- HIPAA (Health Insurance Portability and Accountability Act), including the Final Omnibus Rule
- Health Information Technology for Economical and Clinical Health (HITECH), including Meaningful Use (MU) and Breach Notification
- Sarbanes-Oxley (Financial Accounting)
- Gramm-Leach-Bliley Act (Finance)
- Federal Information Security Management Act of 2002
- (FISMA) and FDA 21 CFR Part 11 (Food and Drugs)
- FERPA (Family Educational Rights and Privacy Act)
- 21st Century Cures Act and TEFCA (Trusted Exchange Framework Common Agreement)
- HIPAA Privacy Rule Updates
- Proposed HIPAA Security Rule Updates*

*Pending approval.



With the dramatic increase in volume of sensitive confidential information in electronic form, various government sponsored security regulations tie together the security and integrity of technological systems and processes. According to Joe Cisna, Director, Vertical Solutions, Global Digital Workplace Healthcare Solutions, US:

"Since its inception in 1996, HIPAA has been the prevailing U.S. law governing patient health information security and confidentiality, and since that time HIPAA has evolved considerably. In parallel, technology has grown in complexity, and unfortunately so have the ambitions and capabilities of bad actors with the intent to breach that technology for nefarious purposes. And while HIPAA is the prominent law as it relates to healthcare, it is far from the only law that impacts healthcare organizations."

In response to these regulations, Konica Minolta is taking the lead in developing and implementing security-based information technologies in Multi-Function Print Devices (MFP - copy, scan, print and fax). Ever since the introduction of the first Konica Minolta MFP, Konica Minolta has strived to develop and implement technologies that safeguard the confidentiality of electronic documents.

Security measures for Konica Minolta MFPs can easily be adopted for use in a wide range of industries, particularly healthcare, where electronic document security is paramount. This requirement will grow more relevant as the trend towards electronic storage and maintenance of sensitive information continues. Whether installed in a small physician practice, a long-term care facility or in a large hospital, Konica Minolta MFPs can provide the confidentiality, integrity and accessibility (also referred to as CIA) that healthcare professionals demand and require.

The combination of increased HIPAA regulatory enforcement as well as sophisticated and targeted cyber attacks have raised the level of risk and priority for appropriately protecting medical information that an organization is trusted with, this includes both covered entities and business associates.

This document will discuss IT related security initiatives and explain how Konica Minolta MFPs, as well as our portfolio of solutions and services, contribute towards HIPAA preparedness strategies to comply with the requirements set forth in HIPAA (including the most recent Final Privacy and Security Rule) and HITECH.

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, aimed to streamline health insurance administration, enhance coverage portability, combat fraud and abuse, and promote medical savings accounts. Title II of HIPAA, known as Administrative Simplification, introduced guidelines to protect the privacy and security of confidential patient data. Over the years, these guidelines have evolved, notably with the introduction of the Privacy and Security Rules in 2003, the HITECH Interim Security Rule in 2009—which included breach notification requirements and penalties—and the Final Rule on Privacy and Security in 2013. HITECH also mandated security risk analyses, including encryption protocols that providers must attest to.

In December 2024, the U.S. Department of Health and Human Services (HHS) proposed significant updates to the HIPAA Security Rule to address the escalating cybersecurity threats in the healthcare sector. This proposal aims to modernize cybersecurity requirements, bridge compliance gaps, and tackle evolving threats with new administrative, technical, and physical safeguards. Key features include mandatory encryption, enhanced access controls, expanded risk analysis requirements, and revised business associate agreement obligations. These updates may require additional investment in regulated entities' cybersecurity and HIPAA compliance programs. In 2023 the Department of Health and Human Services (HHS) released Cybersecurity Performance Goals (CPG) to increase the preparedness of healthcare organizations for cyber threats. These CPGs are now being proposed as potential permanent updates to the HIPAA Security Rule.

The proposed modification, pending approval, would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). Notably, the proposal includes mandatory multifactor authentication, network segmentation to limit intrusion spread, and encryption of patient data to prevent unauthorized access. Additionally, it mandates specific risk analysis practices and compliance documentation. These changes aim to update the HIPAA Security Rule to reflect advances in technology and cybersecurity, ensuring that healthcare providers, health plans, and business associates strengthen their defenses against cyberattacks.

The HIPAA Security Rule defines risk analysis as conducting an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by an entity. Both covered entities (e.g., providers and payers) and business associates must support this exercise with a technical vulnerability assessment. Under the Medicare Promoting Interoperability Program, organizations are required to conduct comprehensive and regular risk analysis, with annual assessments being the best practice. The parameters of the security risk analysis are defined in 45 CFR 164.308(a)(1), which was created by the HIPAA Security Rule.

The 2013 HIPAA Final Rule, also known as the Omnibus Rule, expanded privacy and security protections for health information. It extended compliance liabilities to business associates, updated breach notification requirements, amended the Privacy Rule—including modifications to Covered Entities' Notice of Privacy Practices—and increased civil penalties for breaches. Organizations must be well-prepared to address breach and incident reporting requirements, as non-compliance can result in substantial financial risks.

With the passage of HIPAA, concerns have arisen regarding the security of Multi-Functional Printers (MFPs) and their roles in printing, copying, faxing, and scanning within healthcare settings. Guidance from the Office for Civil Rights (OCR) clarifies that devices like photocopiers and fax machines, which may retain electronic data and potentially store protected health information (PHI), are subject to HIPAA's Privacy and Security Rules. To achieve compliance, healthcare organizations must implement technical, administrative, and physical safeguards to protect the security and integrity of patient information. While no products are officially endorsed as "HIPAA Compliant," it's essential to understand how MFPs can assist organizations in adhering to the HIPAA Security Rule.

Konica Minolta's bizhub MFPs offer a comprehensive suite of security features designed to support healthcare organizations in maintaining compliance with HIPAA regulations. These features include:

Data Encryption: Ensures that all data stored on the MFP's storage device is encrypted, rendering it inaccessible to unauthorized users.

In 2013, Affinity Health Plan, a not-for-profit managed care organization in New York, agreed to a $1.2 million settlement with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) for potential violations of the Health Insurance Portability and Accountability Act (HIPAA). The settlement stemmed from Affinity's failure to erase the hard drives of multiple photocopiers before returning them to a leasing agent. These hard drives contained the electronic protected health information (ePHI) of up to 344,579 individuals.

OCR's investigation revealed that Affinity impermissibly disclosed ePHI by not erasing the data on the copier hard drives. Additionally, Affinity failed to include the ePHI stored on these hard drives in its risk analysis, as required by the HIPAA Security Rule, and lacked proper policies and procedures for returning the photocopiers.

This incident underscores the critical importance of implementing comprehensive data protection measures for all devices handling sensitive information. Healthcare organizations must ensure that all electronic devices, including MFPs, are properly assessed for potential risks and that appropriate safeguards are in place throughout the device lifecycle, especially during decommissioning.

Konica Minolta's bizhub MFPs offer a range of security features designed to assist healthcare organizations in maintaining compliance with HIPAA regulations. These features include data encryption, secure print release, access control, and audit trails, which help protect patient information and mitigate the risk of data breaches.

By leveraging these security features, healthcare providers can enhance their data protection strategies, ensuring that patient information remains secure and that their practices align with regulatory requirements.

Document Tracking:
When enabled, most Konica Minolta bizhub MFPs can track prints, copies, scans and faxes by user name, time of the activity and how many copies were produced. In addition, this can be downloaded electronically from the machine to a desktop computer and imported as a common data file into popular applications such as Microsoft Excel. This feature allows healthcare administrators to track individual usage by who created a document, the name of the file, when it was created, and how many copies were produced. On most bizhub office based products, an administrator can view the actual documents that a user printed, copied, faxed, or scanned.

The HIPAA Security Rule was published on February 20, 2003. The rule details several standard and implementation specifications for Protecting Health Information related to IT, Technology and systems that contain Private Health Information. **Contained in this paper is a list of these Standards and implementation specifications and how Konica Minolta MFP's comply**.

The HIPAA Security regulations are applicable to Electronic Protected Health Information (ePHI) and not for traditional office communications such as facsimile or telephone. As one can imagine, the Standards and Implementation specifications are general in nature and open to interpretation. It is also important to note that many of the Security specifications are not related to Technology but to HR and other areas of compliance. For example, there is a required specification, which calls for workforce sanctions for violations of security policies and procedures. It is also important to know the difference between Required and Addressable specifications:

Required - Measures include workforce sanctions for violations of security policies and procedures, a data backup plan, unique user identification access controls, device and media disposal procedures, and person or entity authentication procedures.

Addressable - Covered entities must first assess whether each addressable specification constitutes a "reasonable and appropriate safeguard" in its environment, based on the specification's likely contribution to protection of electronic PHI. If the entity determines that an addressable implementation specification is reasonable and appropriate, it must implement the measure. If it determines the opposite, then it must document that decision and implement an equivalent alternative measure, if reasonable and appropriate.

The 2003 Security Rule sets forth security standards that define administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic Protected Health Information ("ePHI"). Subpart C of the Security Rule sets forth eighteen security standards that must be implemented through thirteen "required" implementation specifications or twenty-two "addressable" implementation specifications. Although the majority of the Standards do not apply to Digital Office MFPs, we list all of the standards and implementation specifications at the end of this document for the convenience of the reader.

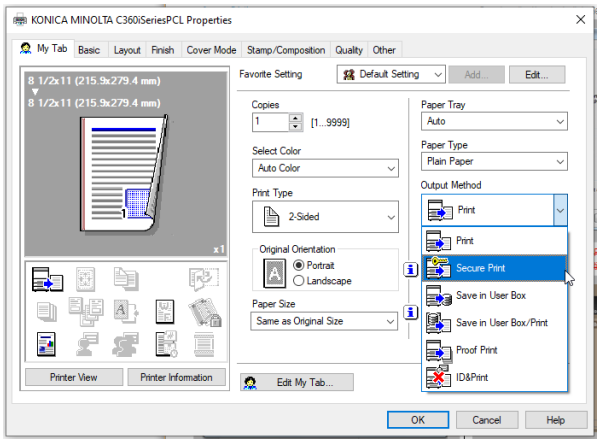
HIPAA Security Standards that are applicable to Konica Minolta bizhub Multi-Functional Machines.
Listed next are Standard features on Konica Minolta bizhub MFPs that satisfy specific HIPAA Security Specifications (the Standards and Specifications are in Blue/Italics):

Access Control, Technical Safeguards
The following functions satisfy the HIPAA Security Specification, Access Control Section Technical Safeguards (Section 164.312): (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec.164.308(a)(4) (ii) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/ or number for identifying and tracking user identity.

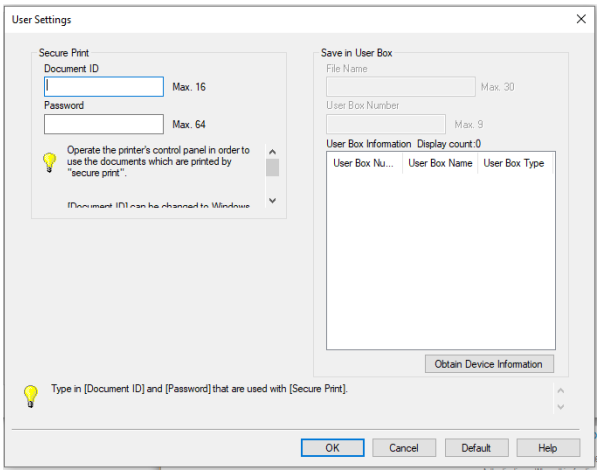
Secure Printing

Konica Minolta MFP's offer a standard feature called Secure Printing. This feature provides to the User sending a print job, the ability to hold the Job in a secure electronic mailbox until that person walks up to the machine and releases the job by inputting a unique, secure, password at the control panel of the MFP. This password is input by the User when they submit a print job from the PC workstation. This process ensures that only the sender of the job can access an electronic document that contains ePHI. In addition, those MFPs equipped with a solid state drive have the ability to store electronic PHI inside the system. When these documents are stored - either by sending them from a PC or by scanning them in at the MFP - users cannot retrieve the document unless a secure password is input at the MFP's control panel.

Below is an example from the bizhub MFP print driver showing the Secure Print Function.



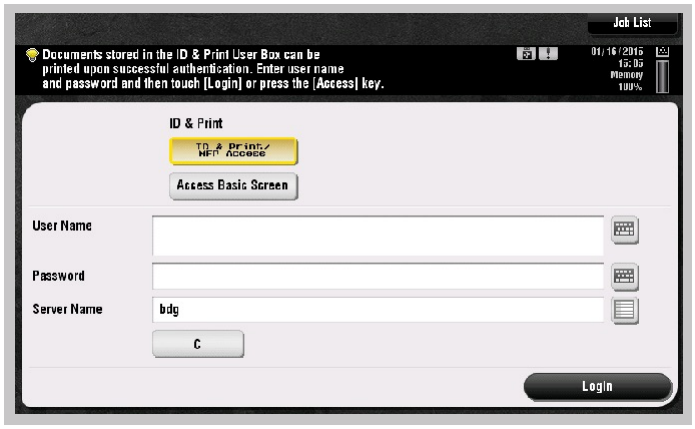
From here the user inputs their Secure Print ID and Password.



User Authentication and Account Tracking

Konica Minolta bizhub MFPs come standard with the ability to enable User Authentication. When this function is enabled, a user is required to input User Name and Password before they are granted access rights to make a copy, send a fax, or perform other functions at the MFP. If a user does not submit or enter the proper credentials, the print job submitted will not be printed. If a user does not enter their ID and password at the copier control panel, they will be denied access rights to the system. When logged in, the user's activities are electronically recorded onto a log file inside the system. Only an Administrator or Key Operator can access this file. This is a very popular feature for many customers, who use this to bill departments and audit individual's copier activities. The User Authentication process can even be connected to Windows Active Directory in real time, which makes User Administration for bizhub MFPs a non-issue for IT personnel.

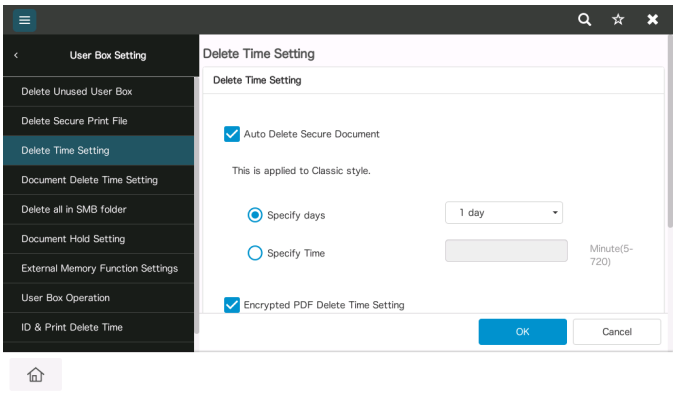
This is an example of the secure User Authentication access screen from the Konica Minolta bizhub MFP control panel:



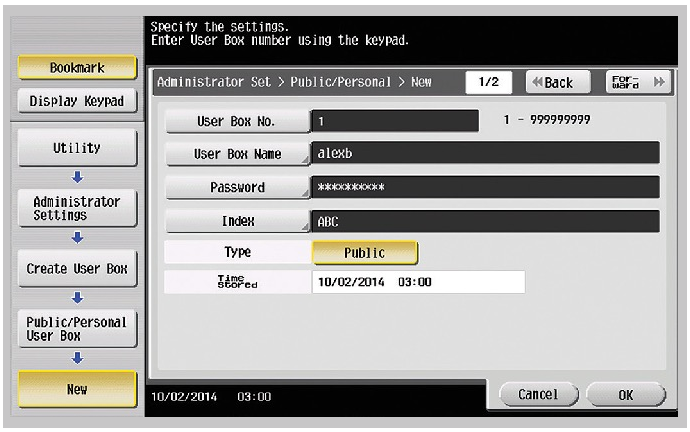
Notice that there are fields to input the User Name, Server Name and Passwords.

When equipped with a solid state drive some Konica Minolta devices support walk up scanning and storage of documents to the MFP's internal hard disk drive. This application is popular for users who would like to store frequently used jobs for later recall and printing. This function is commonly referred to as scanning or printing to a "Mailbox". On Konica Minolta MFPs, mailboxes are password protected. A user must set up a mailbox using a unique password in order for the user to store a job into a mailbox storage folder in the internal hard drive.

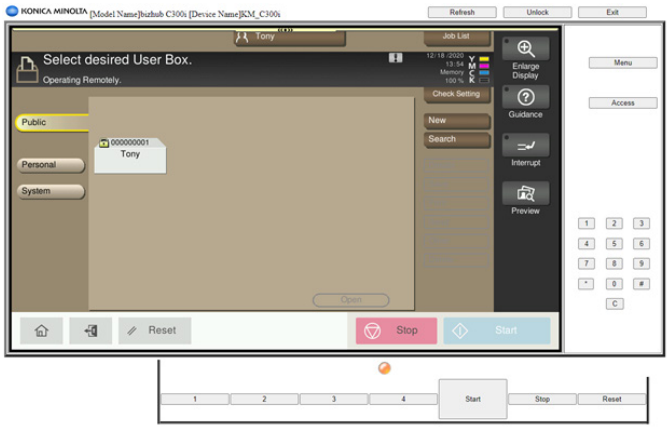
This screen allows the Box Administrator to specify the Auto Deletion time for documents stored in a Box:



This is the set up Box screen – Notice the Password is starred out:



This is a sample screen from the Konica Minolta MFP's control panel showing a Box that was created using the example from above:



When a user wants to recall a scanned or held job, a prompt for password entry will be shown.

Advanced Authentication Technologies

Konica Minolta MFP's offer a standard feature called Secure Print. This feature provides to the User sending a print job, the ability to hold the job in a secure electronic mailbox until that person walks up to the machine and releases the job by inputting a unique, secure, password at the control panel of the MFP. This password is input by the User when they submit a print job from the PC workstation. This process ensures that only the sender of the job can access an electronic document that contains ePHI. In addition to the standard keyboard based authentication log-in methods, Konica Minolta offers advanced technologies for user authentication and identification. One of the main complaints from end users with authentication processes is that it takes too much time and is laborious. An advanced authentication device can provide IT with the security they need and users with the comfort they demand. Currently Konica Minolta offers the following devices for user authentication.

AU-205H – IC Card Reader

Konica Minolta's multi card technology AU-205H takes IC Card authentication to a higher level of security and convenience. The compact AU-205H simultaneously supports HID Prox and Indala®, MIFARE Classic™,MIFARE DESFire™, iCLASS®,iCLASS SE®, iCLASS® Seos™ and iCLASS® Elite Card authentication with secure "ID and Print" operation that saves time and effort – there's no need to enter user name or password, no compromise in print/scan performance, and no loss of the security safeguards you count on to protect sensitive data. Dispatcher Phoenix and Paragon and other Konica Minolta bEST certified applications including Tungsten ControlSuite and PaperCut give you complete authentication and print management solutions with secure pull printing. The AU-205H eliminates the need to manually input a user name and password –and can automatically retrieve data from the any compatible card to emulate keystrokes to obtain access to any supported device. Fast, simple, secure and convenient – that's why bizhub users can count on Konica Minolta.

AU-205H Features for Security and Compliance

Assists in Compliance with Comply with HIPAA Regulations for secure access to print/scan/copy/fax devices in government, healthcare, legal and educational applications.

Secure ID & Print holds print jobs at the MFP until users present their IC Cards – no compromise in security with print jobs containing confidential information waiting in output trays.

Pull Printing (option) enables users to send print jobs to a secure hold queue where they are held until released by presenting the IC Card at any compatible MFP on the network.

Integration with authentication and print management solutions provided by Konica Minolta.

Controlled Access to MFP functions helps reduce unauthorized operation, minimize unnecessary printing, and save paper and energy to support corporate sustainability goals.

As an added convenience to IT, authentication devices can be integrated to Windows Active Directory and Entra ID for seamless user authentication into the existing network user database.

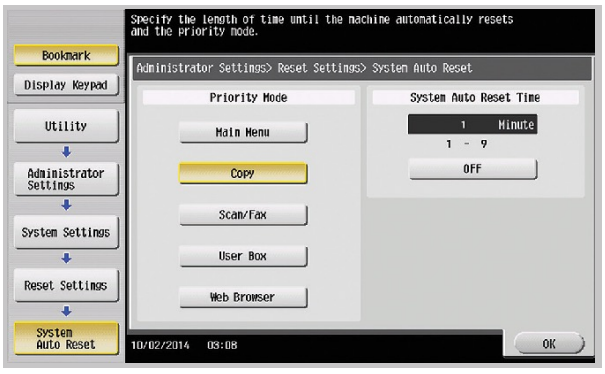
Automatic Reset/Log-off

The following function satisfies the HIPAA Security Specification Section 164.312 (a)(2)(iii): Automatic Log-Off

(A) - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Konica Minolta MFPs can be programmed to automatically reset to a state that requires password input after a predetermined time of inactivity. This ensures that the MFP will reset to a secure state if a user forgets to logoff from an MFP when finished with their session.

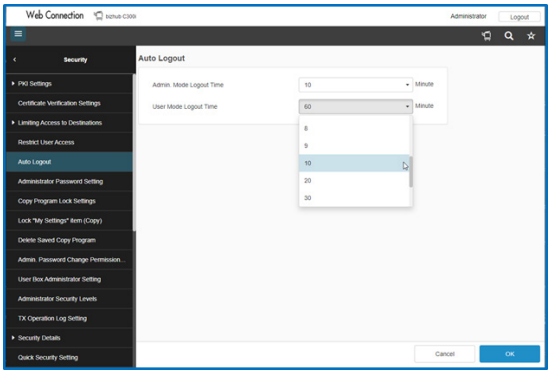
As a walkup electronic distribution device, Konica Minolta MFP's offer the ability to store scanned, faxed and printed documents in a password protected electronic mailbox. To secure this function against user error, Konica Minolta devices can be programmed to automatically reset after a fixed period of inactivity. For example, a healthcare worker logs into an MFP with a unique USER ID password, scans a file to a secure mailbox and walks away forgetting to log out of their session at the device. The MFP would detect no user activity and after 30 seconds reset itself to the password protected log-in state.



bizhub MFP Panel Reset Setting

Notice that the reset timer can be set from 1 to 9 minutes. Some Konica Minolta MFPs can be programmed to reset in as little as 30 seconds. If the machine has the Account Tracking function enabled, the machine will enter a state (after a preprogrammed period of inactivity) that requires a user to enter a unique password. This function should satisfy most concerns about someone forgetting to log off after they are finished scanning or copying documents at the MFP.

This Screen illustrates the Administrator and User Auto Log Off timer setting that is accessible via the MFP's remote Web Browser based interface (Konica Minolta Web Connection.)

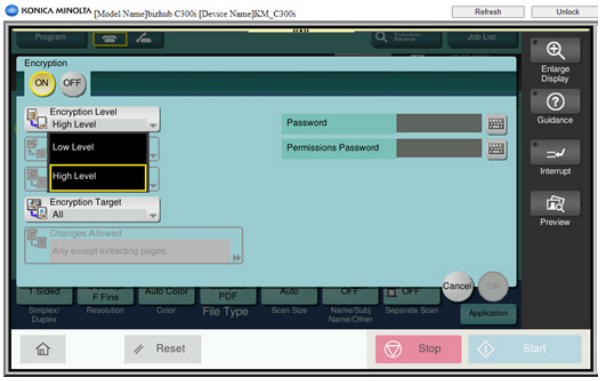


Encryption of Electronic Protected Health Information

The following function satisfies the HIPAA Security Specification Section 164.312 - Technical Safeguards.

§164.312(a)(1) Unique User Identification (R), Emergency Access Procedure (R), Automatic Logoff (A), Encryption and Decryption (A).

bizhub products can encrypt scanned files in PDF format before sending them to a destination across the network. The user has the ability to encrypt a scanned file by selecting the encryption key on the bizhub's control panel. The encryption feature supports the PDF file type, and will require from the recipient of the scan the decryption code to open the file. This feature is very similar to the Adobe Acrobat encryption process where a password is utilized for encryption and opening a file, as well as to access the permissions area of the encryption process.



Physical Safeguards

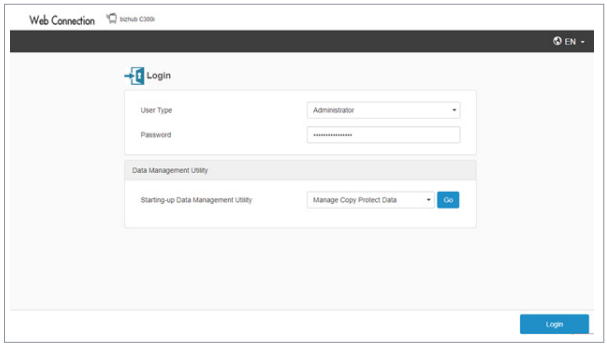
The following function satisfies the HIPAA Security Specification Section 164.310 - Physical Safeguards.

(c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Remote Document Access via MFPs

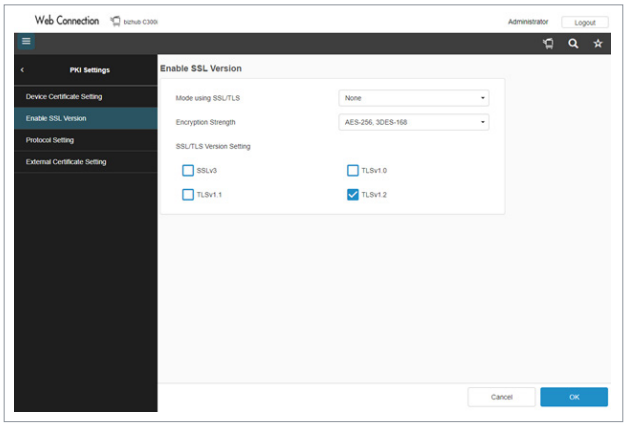
Many Konica Minolta Devices offer the ability to remotely access (via Workstation) print and scanned jobs. This feature can be either disabled or Password protected using a unique alpha numeric code.

This is a sample login screen to a Konica Minolta bizhub's built-in Web Server showing password protection:



Notice the Administrator's Login field. In addition, most bizhub office models offer Kerberos password protection/ encryption. Most Konica Minolta devices support SSL/TLS encryption of data communication between the device and an LDAP Server, Web Connection or PageScope Data Administrator.

This is an example of setting up SSL/TLS via Web Connection on a bizhub MFP.



The following function satisfies the HIPAA Security Specification Section 164.312 Technical Safeguards:

(b) Standard: Audit controls. Implement hardware, software, and/ or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

MFP Audit Logs

Many Konica Minolta bizhub systems contain electronic job logs that record all print, copy, scan and fax jobs sent to or from the MFP. For example, the bizhub MFP Audit Log records all print jobs sent by named users. The Audit Log records when the job was printed, how many copies, the time it was printed etc.

Supported information in the Job Log Include:

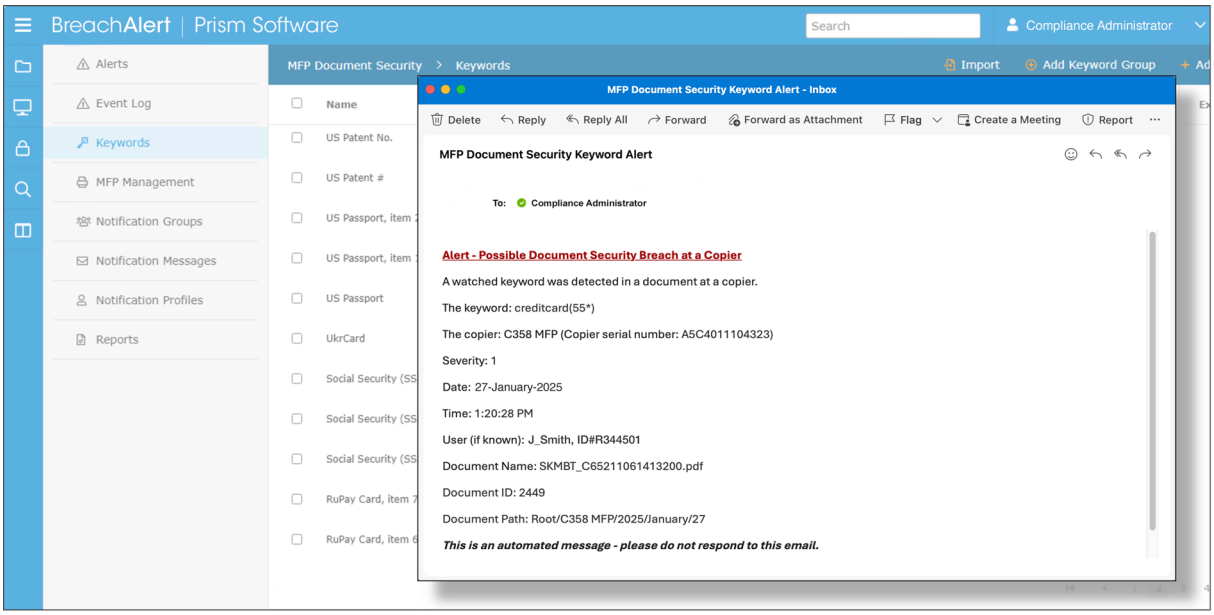
- User ID
- Time & Date of Event
- Job Number
- Job ID
- Job Name
- Scan Destination
- Number of Pages

In addition, Konica Minolta now includes a built-in audit trail security feature in bizhub devices called the Image Log Transfer function. With the Image Log Transfer function, you can transfer the image using the Send-to-FTP or WebDAV process to a registered server at the same time that the device is reading an image in copy mode, reading an image in scan mode, processing a print or image input for FAX RX (reception).

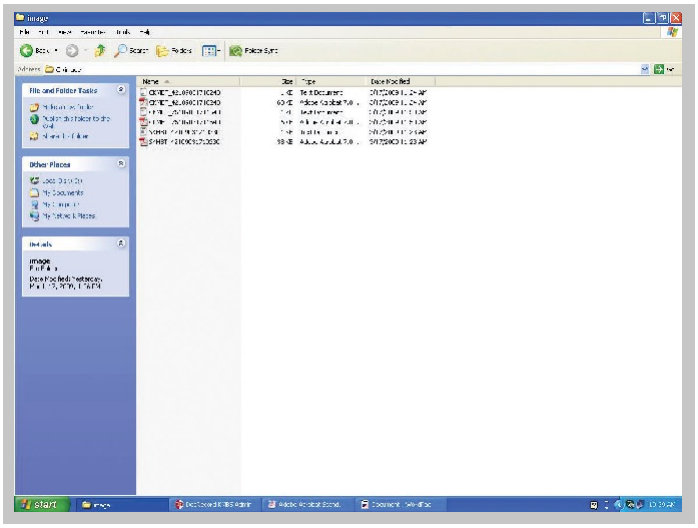
Breach Alert

- bizhub MFP activities are securely archived and accessible only by permitted users
- Automatically records all bizhub MFP activities by user, device, date, and time on supported models.
- Documents are full-text searchable through automatic OCR (optical character recognition)
- Secure and complete content audit trail of supported bizhub MFP activities
- User-configurable key word and key data breach triggers

With this setting enabled all documents, whether electronic originals or paper originals are converted to PDF and sent automatically to a registered external server. Here is an example of a bizhub BreachAlert screen:

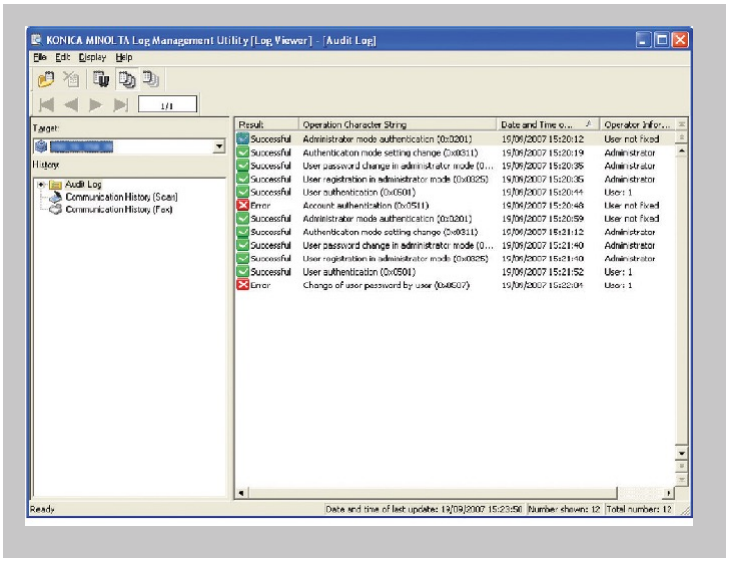


Below is an example of the registered location and the two files that are automatically routed to the external server. The text document is the log file, which is associated with the individual PDF image file of the scanned document.



Authenticated by External Server
<DeviceInformation>
<PrinterSerialNumber>A0R6011901002</PrinterSerialNumber>
</DeviceInformation>
<JobInformation>
<JobID>923</JobID>
<UserName>david</UserName>
<ExtendedSeverName>Servername</ExtendedSeverName>
</JobInformation>
<ImageInformation>
<SendTime>090323082540</SendTime>
<FileName>CKMBT_42109031809400.pdf</FileName>
</ImageInformation>

Konica Minolta also provides, at no charge, an application called the Log Management Utility. The Log Management Utility enables a company to keep long-term records of completed jobs. It provides an audit log that not only covers a long period of time, but one that can be reviewed at any time and can be searched easily and efficiently. This utility also allows the logs of multiple MFPs to be centrally managed. This is a sample log captured from a bizhub MFP:



Physical Safeguards

The features explained below satisfy various requirements under Physical Safeguards, Section 164.310 (d)(1): Standard: Device and media controls.

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

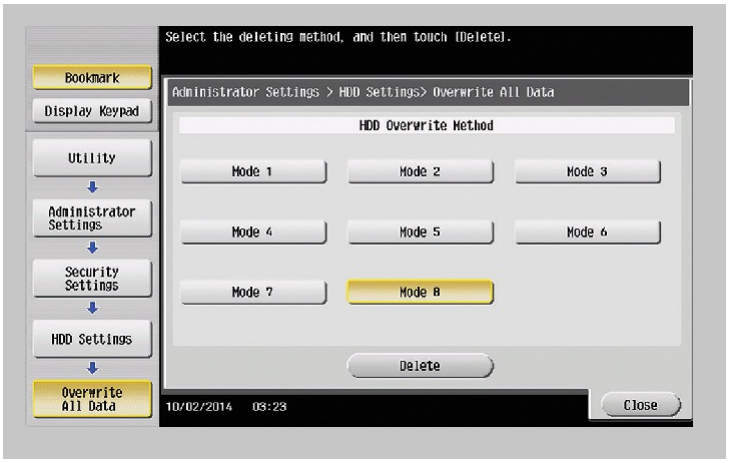
Implementation specifications:

(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

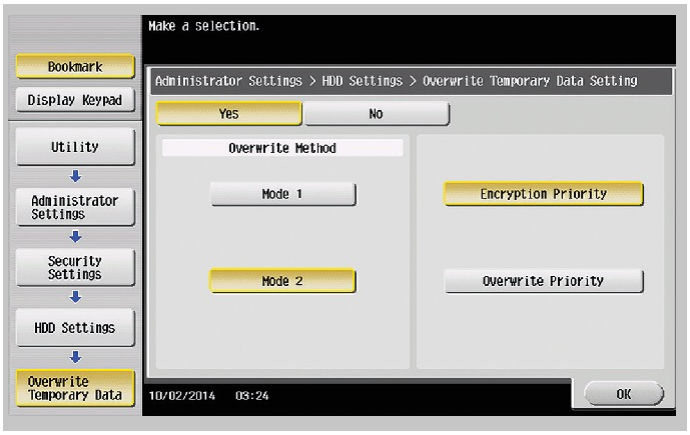
(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Storage Media Sanitize and Overwrite

When equipped with a hard disk drive (HDD), Konica Minolta MFPs can store ePHI. The data is erasable (deleted) by users who own the documents that reside inside the MFP's HDD (inside Password Protected Mailboxes). For added security, an Administrator or Technician can physically format (erase) the HDD if the MFP needs to be relocated. The hard drives can be overwritten (sanitized) using a number of different methods conforming to military specifications. In addition, Administrators can program the bizhub to automatically overwrite any temporary data remaining on the HDD on a per job basis. Overwritten image data includes documents deleted from electronic User Box's, Secure Print Box's etc. NOTE: for HDD MFP's Only. This is not required for SSD MFP's.



This configuration is from the bizhub MFP's Security



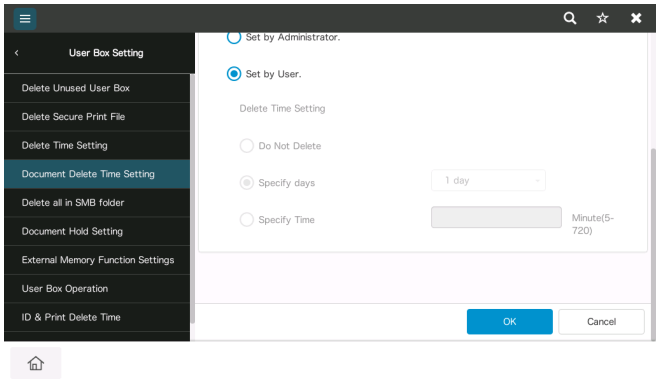
Automatic deletion of electronic files from Konica Minolta bizhub MFPs

Many healthcare Security professionals are concerned about scanned ePHI residing on the MFPs hard drive. Most people need to use the scanning functionality of the MFP, however, they are concerned about the risks. As mentioned before, ALL held jobs in User Boxes can be password protected. In addition, bizhub MFPs can be programmed to automatically delete held jobs at pre-determined intervals.

This is the setting to automatically delete the job on a Konica Minolta bizhub MFP.

Device and Media Controls, Accountability and Data Backup and Storage

Konica Minolta document management software solutions can assist a Covered Healthcare Entity comply with the following standards: (d)(1) Standard: bizhub SECURE Healthcare Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. (2) Implementation specifications: (iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore. (iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.



KONICA MINOLTA SOLUTIONS FOR BACKUP STORAGE, ARCHIVAL AND RETRIEVAL OF ELECTRONIC PROTECTED HEALTH INFORMATION

Document and Enterprise Content Management

Konica Minolta provides an array of document and Enterprise Content Management (ECM) solutions via our BlueIrisIQ division. Our ECM solutions maintain all document content from scanned images to electronic documents, forms and multiple file formats, and provide intelligent form recognition based on business application usage, workflow rules and unmatched integration with virtually any HIS/EHR or back office system.

Capture Documents

Konica Minolta provides an array of high speed, integrated, scan-to-EHR with HL7 CDA capabilities to support interoperability initiatives and reduce workflow inefficiencies typically associated with patient record scanning processes.

Secure, EHR-Integrated Scanning, Cloud Fax and Direct Messaging

The Konica Minolta Healthcare-Enabled MFP, Connected by Kno2, enables our customers with a secure and electronic means of exchanging Protected Health Information (PHI) via Direct Secure Messaging, HIPAA-Compliant Cloud Fax, as well as EHR-integrated scanning to popular extended care systems, such as PointClickCare, MatrixCare, Wellsky and Yardi.

All Covered Healthcare IT and Compliance Services

HIPAA compliance begins with a risk assessment of the healthcare organization, and is a requirement of every healthcare provider. Our All Covered Healthcare compliance team assists our customers with the persistent security and compliance challenges by collaborating on a comprehensive threat assessment to protect data without straining staff or budget. Included in these services are HIPAA Risk Assessments, ongoing compliance capabilities and a variety of security services.

Secure Print Release

Konica Minolta provides tight integration into host-based EHRs, such as Epic and Cerner, enabling our customers with the ability to securely release printed PHI at networked printers, and reduce the potential for HIPAA breach exposure.

bizhub SECURE Healthcare

Advanced security settings performed by a Konica Minolta professional service team member advances compliance efforts significantly. bizhub SECURE Healthcare provides a robust schedule of settings to include:

- 20-digit secure alphanumeric password to lock down your bizhub storage media drive
- Encrypting the entire contents of your bizhub storage media Drive for remarkable data security
- Eliminating any trace of data even after it's deleted with Temporary Data Overwrite (TDO conforms to DoD methods). This only applies to MFP's with HDD's. i-Series MFP's no longer utilize this feature based on the architecture of a solid state drive (SSD).
- Timing your bizhub MFP to auto-delete any material located in personal or public user boxes, system user boxes, documents and folders
- Disabling insecure services, protocols and ports at the MFP
- Enabling SSL/TLS on the MFP (Self-Sign Certificate)

Security Measures

Konica Minolta MFPs can easily be adopted for use in the healthcare industry and will grow more relevant as the trend towards electronic storage and maintenance of protected healthcare information continues. Whether installed in a small office as workgroup device or in a large hospital as a departmental workhorse, Konica Minolta bizhub MFPs can provide you with the security, reliability and stability that healthcare professionals demand and require.

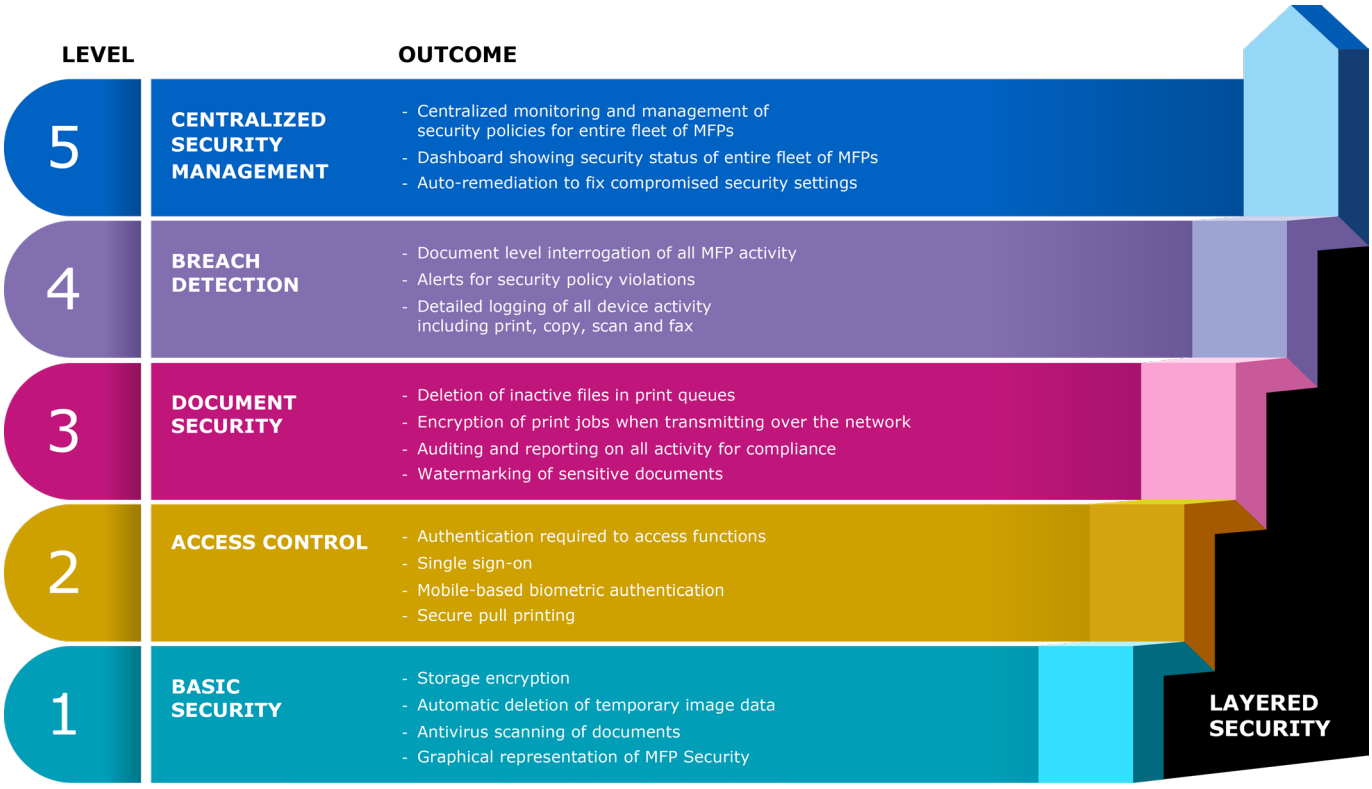
HIPAA Conclusion

With the dramatic increase in volume of protected health information in electronic form, HIPAA privacy requirements tie together the security and integrity of technological systems and processes. Technology security has become critically important as covered entities use their electronic systems to comply with HIPAA regulations. With the growing popularity of network-connected multifunctional products, people in the healthcare industry will increasingly look to MFPs as an efficient and cost effective method of distributing, storing and receiving ePHI. Security measures for Konica Minolta MFPs can easily be adopted for use in the healthcare industry and will grow more relevant as the trend towards electronic storage and maintenance of protected healthcare information continues.

Konica Minolta's Layered Security Approach

Any breach or mishandling of PHI can lead to severe consequences—both in terms of fines and loss of patient trust. Many healthcare providers may not realize that printers, scanners, and copiers are often vulnerable points in their data security strategy.

Konica Minolta bizhub MFPs offer a **multi-layered approach** to security, specifically designed to meet healthcare industry standards and regulations to safeguard your organization and patient data across all phases—whether it's being scanned, printed, stored or shared with your referral sources. The following security model outlines recommendations your organization should consider regarding your office technology:



HIPAA Conclusion

With the dramatic increase in volume of protected health information in electronic form, HIPAA privacy requirements tie together the security and integrity of technological systems and processes. Technology security has become critically important as covered entities use their electronic systems to comply with HIPAA regulations. With the growing popularity of network-connected multifunctional products, people in the healthcare industry will increasingly look to MFPs as an efficient and cost effective method of distributing, storing and receiving ePHI. Security measures for Konica Minolta MFPs can easily be adopted for use in the healthcare industry and will grow more relevant as the trend towards electronic storage and maintenance of protected healthcare information continues.

HIPAA Security Rule: Summary of Safeguard Standards and Implementation Specifications The HIPAA Security Rule establishes a framework of administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI). Each safeguard standard is supported by implementation specifications, designated as either Required (R) or Addressable (A), depending on their implementation specification.

Standard	Section	Implementation Specification (R)=Required, (A)=Addressable
ADMINISTRATIVE SAFEGUARDS		
Security Management Process	§164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	§164.308(a)(2)	(R)
Workforce Security	§164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	§164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	§164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	§164.308(a)(6)	Response and Reporting (R) Data Backup Plan (R)
Contingency Plan	§164.308(a)(7)	Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	§164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	§164.308(b)(1)	Written Contract or Other Arrangement (R)
PHYSICAL SAFEGUARDS		
Facility Access Controls	§164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	§164.310(b)	(R)
Workstation Security	§164.310(c)	(R)
Device and Media Controls	§164.310(d)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
TECHNICAL SAFEGUARDS		
Access Control	§164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	§164.312(b)	(R)
Integrity	§164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A) (R)
Person or Entity Authentication	§164.312(d)	Integrity Controls (A)
Transmission Security	§164.312(e)(1)	Encryption (A)

Count On Konica Minolta

Konica Minolta Business Solutions U.S.A., Inc., is an industry leader in advanced digital imaging systems for business, professional and institutional organizations. With in-depth knowledge of workflow needs and productivity demands in a wide range of specialized applications, Konica Minolta provides right-size solutions for color and B&W printing and scanning from desktop to print shops. Konica Minolta also offers advanced technology in color reproduction, print control, security capabilities, and flexible networking to help end-users improve output and control costs.

With over 37,000 worldwide employees, cutting-edge research programs in optical and digital technology, a deep commitment to environmental protection, and the industry's most complete line of document imaging systems, Konica Minolta was recognized by Brand Keys for the second consecutive year as the #1 Brand for Customer Loyalty in the MFP Office Copier Market. As long as you count on Konica Minolta, you've made the right decision.

Legal Disclaimer

This paper is for general informational purposes only and does not represent legal advice or a legal opinion. Because of its generality, it may not be applicable to your specific situation. For legal advice, you should consult with legal counsel or HIPAA Compliance Officer regarding your own particular legal needs. NOTE: Some of the specific security features and options described in this report may only apply to certain Konica Minolta models. It is best to refer to the documentation that is provided with every Konica Minolta bizhub MFP to verify exactly which security features are included with a specific machine. It is also important to note that a specific machine may require an upgrade to achieve and/or enable some of the features discussed in this report. Please refer to your service representative for further information. This paper is current as of April 2025.

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446
CountOnKonicaMinolta.com

Item #: HPA_HTC_WP
10/2025-X