HIPAA Security Compliance for Konica Minolta bizhub MFPs
Table of Contents

Introduction ........................................................................................................... 1
What is HIPAA?..................................................................................................... 1
HIPAA Security Standards that are applicable
to Konica Minolta bizhub Multi-Functional Printers ........................................ 2
Access Control ................................................................................................. 2
Secure Print ......................................................................................................... 2
User Authentication & Account Tracking ............................................................ 3
Advanced Authentication Technologies ............................................................. 4
Auto Reset/Logoff ............................................................................................... 5
Encryption of Electronic Protected Health Information ........................................ 6
Password Protection .......................................................................................... 6
Event/Audit Log ................................................................................................. 7
Hard Drive Sanitize and Overwrite ...................................................................... 8
Device and Media Controls, Accountability and Data Backup and
Storage ................................................................................................................ 9
Conclusion ......................................................................................................... 10
HIPAA Security Final Rule –
Appendix A to Subpart C of Part 164 – Security Standards: Matrix .............. 11

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 documentation 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

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

- HIPAA (Health Insurance Portability and Accountability Act)
- Sarbanes-Oxley (Financial Accounting)
- Gramm-Leach-Billey Act (Finance)
- Federal Information Security Management Act of 2002 (FISMA) and FDA 21 CFR Part 11 (Food and Drugs)
- ISO 15408, also known as, Common Criteria

In response to these regulations, Konica Minolta is taking the lead in developing and implementing Security based information technologies in Multi-Function office machines. 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.

With the rising popularity of network connected Office Machines for printing and scanning, people in various industries will increasingly look to MFPs as an efficient and cost-effective method of distributing, storing and receiving sensitive electronic information. Security measures for Konica Minolta MFPs can easily be adopted for use in a wide range of industries where electronic document security is important. This requirement will grow more relevant as the trend towards electronic storage and maintenance of sensitive information continues. Whether installed in a small office as a workgroup device or in a large hospital as a departmental workhorse, Konica Minolta MFPs can provide the security, reliability and stability that healthcare professionals demand and require.

This document will discuss IT related security initiatives and explain how Konica Minolta MFPs comply with the various rules and regulations set forth in HIPAA (Health Insurance Portability and Accountability Act) legislation.

What is HIPAA?

HIPAA is a law passed by Congress in 1996, its intention is to protect basic personnel information related to healthcare privacy. The law was also intended to streamline healthcare document management practices by providing a set of rules for electronic document management, related to the privacy of the patient and the accountability of the healthcare provider.

With the passage of HIPAA, healthcare related facilities are concerned about HIPAA regulations and how they apply to the security of Multi-Functional Printers (MFP) printing, copying, faxing and scanning functions in the office. In addition to the healthcare industry, many organizations are aware of this emerging trend for electronic document storage, and are concerned about security issues related to electronic document distribution.
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.

The final 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 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 below 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).

(2) 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 hard 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 copier - users cannot retrieve the document unless a secure password is input at the copier’s control panel.

Below is an example from the bizhub 361 print driver showing the Secure Print Function.

[Image of Secure Print Function]
From here the User inputs their Secure Print ID and Password.

This is an example of the secure User Authentication access screen from the Konica Minolta bizhub C452 control panel:

This is an example of the control Panel of the Konica Minolta bizhub 421 where there is a “Secure Print” waiting to be released:

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

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

When a user wants to recall a scanned or held job, he/she is presented with the password entry screen:

Advanced Authentication Technologies

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-101 & the AU-102 Biometric Finger Vein Readers

The AU-101/AU-102 is the only biometric finger vein reader which connects directly to the MFP and works in conjunction with the machine’s internal authentication capabilities or integrates with Konica Minolta’s PageScope Enterprise Suite. A user simply walks up to an MFP and places his or her registered finger in the AU-101/AU-102 to gain access to the MFP to complete copy, scan and fax functions.
Secure printing has never been easier than with the “ID and Print” feature. A user sends a print job to the MFP where it is held until the user is in front of the MFP. To release their job, the user simply places his or her registered finger in the AU-101/AU-102 without any other interaction.

The AU-101/AU-102 allows a user to:
1. Walk up to an MFP
2. Place registered finger on the AU-101/AU-102 reader
3. Begin the copy/fax/print/scan functions

- The AU-101/AU-102 offers the “ID & Print” feature
- Integrates with PageScope Enterprise Suite
- Authentication Manager, Authentication Unit Gateway (AUG) required, to offer a complete authentication and accounting solution with custom control panel based on a user finger vein pattern.

AU-201H – HID Proximity Card Reader

The AU-201H is an HID Proximity card reader which connects directly to the MFP and works in conjunction with the machine’s internal authentication capabilities or integrates with Konica Minolta’s PageScope Enterprise Suite and Konica Minolta exclusive bEST Equitrac Office and Equitrac Express integrated solutions. The user simply walks up to an MFP and places their card near the reader to gain access to the MFP to complete copy, scan and fax functions. Secure printing has never been easier than with the “ID and Print” feature. A user sends a print job to the MFP where it is held until the user is in front of the MFP. To release their job, the user simply places their HID card near the AU-201H to release only their documents without any other interaction. The AU-201H is compatible with most existing HID Proximity card formats currently being used by our customers or Konica Minolta offers HID Proximity cards as a turn key solution.

The AU-201H allows a user to:
1. Walk up to an MFP
2. Place their HID Proximity Card near the AU-201H
3. Begin the copy/fax/print/scan functions

- The AU-201H offers the “ID and Print” feature
- Integrates with PageScope Enterprise Suite Authentication Manager to offer a complete authentication and accounting solution with custom control panel based on HID Card Authentication.

As an added convenience to IT, all 3 authentication devices can be integrated to Windows Active Directory 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.

bizhub C552 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 (PageScope Web Connection).
Encryption of Electronic Protected Health Information

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

bizhub OP based 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.

Password Levels to access documents on MFPs from remote workstations

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 (Secure Socket Layer) encryption of data communication between the device and an LDAP Server, PageScope Web Connection or PageScope Data Administrator.

This is an example of setting up SSL via PageScope Web Connection on a bizhub C552:
Audit Controls

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 new built-in audit trail security feature in bizhub OP devices called the Image Log Transfer function. With the Image Log Transfer function, you can transfer the image using the Scan-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).

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 scanned job captured and sent to the external log server:

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.
Konica Minolta also provides at no charge an application called the Job Log Manager 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 C552:

Physical Safeguards

The features explained below satisfy various requirements under Physical Safeguards, Section 164.310:

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.

(2) 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.

Hard Drive 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 (erases) 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.

This configuration is from the bizhub C360’s Security Mode Panel.
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 C552

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: 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

Introduction

Konica Minolta sells Prism Software’s DocRecord® software application. It has been specially developed to work seamlessly together with Konica Minolta bizhub MFPs. DocRecord electronically archives documents for quick electronic retrieval by either local or Internet users. Individuals can utilize Konica Minolta bizhub MFPs to scan hard copy documents and automatically deliver them to DocRecord, which then converts them into electronic documents that are instantly accessible to all users. When installed in a healthcare environment DocRecord can satisfy an important HIPAA requirement under the Device and Media Controls section – Data backup and storage. DocRecord provides extensive backup, storage and retrieval of ePHI.

Capture Documents

Documents can be entered into DocRecord through a number of sources - scan directly from the bizhub multi-function printer (MFP), from a production scanner (for heavy duty scan requirements), through eCopy™, from e-mail capture, or directly from the desktop. File documents directly into DocRecord from Microsoft Word, Excel, PowerPoint, and Outlook. Documents can be entered individually or in batches. DocRecord has a number of tools that expedite the simple and efficient batch scanning and filing of documents – such as generating barcoded cover sheets for automatic indexing and filing, splitting up a mixed batch of different document types, or splitting a batch scan of similar documents into a single document.

Index and Store Documents

DocRecord can perform a variety of process functions for documents. These functions include optical character recognition (OCR) that converts a scanned image into a text document, automatically assigns indexing information, converts the file type into a TIFF or PDF, and much more. OCR can be performed for a full page, selected regions, indexing “zones,” or for barcodes. Once completed, documents are auto-filed into the correct folders within DocRecord. These folders are created prior to document filing or can be automatically created for incoming documents.

Search, Retrieve, and View Documents

Once documents are stored in DocRecord, they are available for searching and retrieving by others. Searches can be done locally by users (from the DocRecord Client) on the network or remotely through an Internet browser (on the DocRecord Web Client). Searches can be as simple, advanced, or custom as required. You can also view related documents through DocRecord’s powerful cross reference capability. Returned documents are then displayed in the interface with a preview of the selected document. View over 300 document types.
Secure Documents
DocRecord provides a highly secure document system that uses Windows security. Permissions and restrictions are based upon existing Active Directory groups and users. Audit trails are available to track document events such as check-in and check-out, forwarding, modifications, deletions, and more. Version control, versioning history, and roll-back to prior versions can be easily accomplished with DocRecord.

Storage of Documents
Unlimited storage capacity — access unlimited storage space by moving documents to any Windows or network operating system storage device — such as a NAS (network attached storage), DVD, DVD Jukebox, and other storage devices. These features provide an easy way to backup and restore systems even during emergencies. Documents can be stored on DVDs and secured in remote safe locations.

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. 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.

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 Healthcare Security Officer regarding your own particular legal needs. This paper is current as of October 1, 2009.

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.
(a) General requirements. Covered entities must do the following:
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4) Ensure compliance with this subpart by its workforce.
(b) Flexibility of approach.
(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
(2) In deciding which security measures to use, a covered entity must take into account the following factors:
(i) The size, complexity, and capabilities of the covered entity.
(ii) The covered entity’s technical infrastructure, hardware, and software security capabilities.
(iii) The costs of security measures.
(iv) The probability and criticality of potential risks to electronic protected health information.
(c) Standards. A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.
(d) Implementation specifications. In this subpart:
(1) Implementation specifications are required or addressable. If an implementation specification is required, the word “Required” appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word “Addressable” appears in parentheses after the title of the implementation specification.
(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.
   (i) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must—
      (I) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s electronic protected health information; and
     (ii) As applicable to the entity—
        (A) Implement the implementation specification if reasonable and appropriate; or
        (B) If implementing the implementation specification is not reasonable and appropriate—
   (1) Document why it would not be reasonable
(2) Implement an equivalent alternative measure if reasonable and appropriate.
(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

§ 164.308 Administrative safeguards.
(a) A covered entity must, in accordance with § 164.306:
(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.
(ii) Implementation specifications:
(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
(ii) Implementation specifications:
(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
(4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) Implementation specifications:
(A) Isolating healthcare clearinghouse functions (Required). If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.

(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement:
(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:
(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.
(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.

(b)(1) Standard: Business associate contracts and other arrangements. A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to—

(i) The transmission by a covered entity of electronic protected health information to a healthcare provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met.

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§ 164.310 Physical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
(iii) **Access control and validation procedures (Addressable).** Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) **Maintenance records (Addressable).** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) **Standard: Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

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

(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.

(2) **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.
   (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.

§ 164.312 Technical safeguards.

**A covered entity must, in accordance with § 164.306:**

(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 § 164.308(a)(4).

(2) **Implementation specifications:**
   (i) **Unique user identification (Required).** Assign a unique name and/or number for identifying and tracking user identity.
   (ii) **Emergency access procedure (Required).** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
   (iii) **Automatic logoff (Addressable).** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
   (iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.

(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.

(c)(1) **Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) **Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) **Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) **Implementation specifications:**
   (i) **Integrity controls (Addressable).** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
   (ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
Count On Konica Minolta

Konica Minolta Business Solutions U.S.A., Inc., is a fast-growing 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 shop. 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.