WHITE PAPER

eCopy and the Health Insurance Portability and Accountability Act (HIPAA)

NUANCE

Contents

Extensive use of the Internet for gathering and distributing information has led to heightened levels of concern over personal privacy.

Although healthcare providers have a long tradition of respect for individual privacy, consumers want assurances that their personal health information remains accessible only to those with a legitimate need to see it.

In response to these concerns, and to facilitate more widespread use of Internet technologies in all aspects of healthcare, the Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996. As its name suggests, the bill guarantees health insurance portability when workers switch jobs. It also includes sweeping provisions to ensure the security and privacy of patient health information.

Since its enactment, government bodies have been busy putting together a series of regulations for organizations that use or have access to patient health information. Some of these regulations are already in effect, while others will become law soon.

When the transfer of patient health information is involved, organizations must ensure that HIPAA's privacy and security regulations are adhered to at all times.

eCopy's document distribution and integration solution offers healthcare organizations unique opportunities to streamline business practices, reduce administrative overhead, and improve communication with business partners and consumers. eCopy products make it quick and easy to deliver digital copies of paper documents across internal computer networks or the Internet.

Becoming HIPAA compliant is a task of enormous magnitude for most healthcare organizations. It requires careful examination of existing business practices and technical infrastructure, and may require significant changes in the way healthcare providers conduct business. This document does not attempt to examine the broader aspects of HIPAA compliance, but instead examines the implications of HIPAA's privacy and security rules on digital document distribution using eCopy's products. We hope that after reading this document you will have a better idea of how eCopy can help you achieve cost savings and improve organizational effectiveness while complying with these regulations.

Disclaimer

The information in this document outlines the main requirements of HIPAA regarding the handling of patient health information as interpreted by eCopy, Inc. This material should not be regarded as a definitive statement of HIPAA regulations or as a way to achieve compliance.

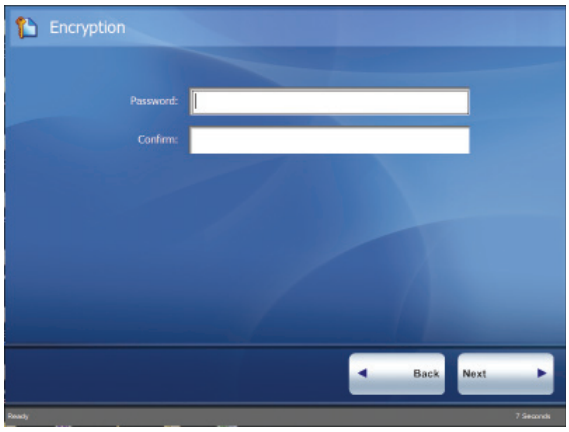
Terms used in this document

The following terms are often used in HIPAA-related discussions and are used throughout this document:

- Patient Health Information (PHI): Any information gathered during the registration, diagnosis, or treatment of a medical condition.
- Covered Entity (CE): Any entity that handles patient health information, including providers, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.

About eCopy

eCopy is an innovative provider of open and flexible solutions that rapidly integrate paper-based information into existing business processes and applications.



Numerous industries including legal, healthcare, and financial services use eCopy to easily access, modify, distribute, and share information to add value to their business

The Health Insurance Portability and Accountability Act (HIPAA) includes wide-ranging provisions that aim to:

- Guarantee health insurance portability
- Protect patient health information against unauthorized access
- Simplify the electronic transfer of medical information

The bill was signed into law in 1996 and since then the Department of Health and Human Services has established a set of rules that relate to the transfer and protection of health information as defined under HIPAA. These rules collectively fall under the heading "Administrative Simplification." There are four rules, two of which have significant implications regarding the distribution of paper-based medical information across computer networks:

Privacy Rule

This rule requires CEs to take all reasonable measures to ensure the confidentiality, integrity, and availability of individually identifiable patient health information. It applies not just to electronic information, but also to paper and oral information. The Privacy Rule was finalized in August 2002 and became effective for all health plans and healthcare providers in April 2004.

Security Rule

This rule sets standards to provide a uniform level of protection for all health information that is stored or transmitted electronically. It also includes proposals for the use of electronic signatures. This rule was finalized in February 2003. Most health plans and healthcare providers were required to comply with HIPAA privacy requirements by April 2005.

The other two Administrative Simplification rules facilitate the electronic exchange of medical data by mandating a single standard to replace the numerous incompatible standards that have evolved:

Transaction and Code Set Rule

This rule standardizes the formats and protocols used for electronic data interchange (EDI). EDI allows medical, billing, and other information to be exchanged and processed quickly and cost effectively. This rule became effective October 2000.

Identifier Rule

This rule proposes standards for National Standard Health Care Providers, National Standard Employers, and National Health Plan identifiers. This rule became effective July 2002.

About HIPAA compliance

Organizations achieve HIPAA compliancy by enforcing policies and procedures that safeguard the privacy and security of patient health information. Technology can help an organization become HIPAA compliant, but no product can be labeled "HIPAA compliant." This document identifies the elements of eCopy's document distribution technology that can help organizations comply with HIPAA's Administrative Simplification requirements when distributing patient health information electronically.

Background

The Privacy Rule went into effect for all healthcare organizations in April 2004. CEs are obligated to implement appropriate administrative, technical, and physical safeguards to protect the privacy of patient health information, whether in electronic form or not. At the same time, CEs must make sure that the information is readily available to those with a legitimate need to see it.

The rule does the following:

- Limits the non-consensual use and release of private health information
- Gives patients new rights to access their medical records and to know who else has accessed them
- Restricts most disclosure of health information to the minimum needed for the intended purpose
- Establishes new criminal and civil sanctions for improper use or disclosure
- Establishes new requirements for access to records by researchers and others

The Privacy Rule affects the way all healthcare organizations conduct business. At a minimum, CEs must carefully examine existing policies and procedures to ensure that they do not violate the new rules. Smaller medical offices may need to make adjustments to their facilities to minimize access to patient health information, such as isolating and locking file cabinets or records rooms, or providing additional security such as passwords on computers maintaining personal information. Larger organizations may need to adopt broad, new privacy policies and modify existing technical infrastructures, especially if their patient records are already in electronic form. All organizations must take whatever measures are necessary to promote a more privacy-conscious environment.

Sharing patient health information using eCopy

eCopy's products make it easy to incorporate paper-based patient information into various electronic medical records (EMR) systems. During this information capture and electronic filing process, CEs must implement safeguards to ensure that privacy is maintained at all times. For the most part, these safeguards are procedural issues rather than technical issues – the same safeguards must be in place if you are using a standalone fax machine or making a photocopy for delivery to another location. eCopy's products offer several features that make it easier to implement these safeguards.

E-mailing or faxing

When e-mailing or faxing clinical information using eCopy products, the following privacy safeguards are available:

- The sender must authenticate him/herself, making it impossible to send information anonymously.[1]
- A copy of the message is delivered to the sender's e-mail inbox or Sent Items folder. This provides a record of what was sent and to whom, making it easier to document disclosures.[2]
- Optional 128-bit encryption of file attachments helps patient health information remain confidential.
- eCopy's Quick Connect feature can easily automate the workflow process for scanned patient health information by integrating with medical record management systems.
- On Lotus Notes-based systems, you can save a copy of all outbound messages with external addresses on the Notes server.
- eCopy maintains a transaction log of all eCopy scanning activity. The administrator can configure one or more tracking information fields that must be filled in before the message is sent.
- By sending patient health information by e-mail rather than fax, you ensure that it is delivered to a private e-mail inbox rather than to a public fax machine where it can be viewed by anyone.

Note that electronic communication of patient health information is subject to additional constraints based on requirements in the Security Rule. These are covered later in this document.

Scanning to Desktop

eCopy's Scan to Desktop function delivers scanned documents to the authenticated user's personal Scan Inbox. This function also includes features to safeguard the privacy of scanned health information:

- eCopy software can be configured so users can only deliver documents to their own scan inbox. This limits the possible distribution of patient health information.
- eCopy uses the security features of the network operating system to ensure that only the owner can retrieve scanned documents from his/her Scan Inbox.

Note that security must be in place at the desktop to ensure that the user's PC is not left logged-on when unattended, but this is an administrative rather than a technical issue.

Using eCopy Quick Connect

eCopy Quick Connect delivers scanned documents to a network folder or FTP site, from where they can be retrieved by authorized individuals or workflow applications. Administrators can easily configure the destination folders so that they are only accessible to users who are authorized to view patient health information.

Minimum disclosure

The HIPAA Privacy Rule requires CEs to take reasonable steps to limit the disclosure of patient health information to the minimum necessary to accomplish the intended purpose. Although treatment-related disclosures are specifically exempted from this requirement, this still leaves many other disclosure relationships where providers and other CEs must limit the information that is released.

Where patient information is retained on paper or has been previously scanned into a document management system, eCopy Desktop, the application used to view scanned documents, provides features to limit the disclosure of information:

- Drag-and-drop e-mail and fax capability lets you select which pages of the patient's record to send.
- Markup tools let you "whiteout" or "blackout" certain personal information before delivering it to a third party.

Using these features help ensure that the recipient sees only the relevant portions of the record.

Transferring information internally

Large healthcare providers frequently need to transfer patient health information internally between different departments (for example, surgery, pharmacy, records department, etc.). This is often done using runners or vacuum tubes.

Security Rule

Background: The Security Rule defines standards to provide a uniform level of protection for all health information that is stored or transmitted electronically.

The Security Rule mandates a combination of administrative and technical measures to ensure the integrity, confidentiality, and availability of electronic data. These are presented in four categories:

Administrative procedures: These are documented, formal processes to manage the implementation of security measures and the conduct of personnel in relation to the protection of data.

Physical safeguards: These relate to the protection of computer systems and equipment from fire and other hazards, as well as from intrusion. Physical safeguards include the use of locks and other measures to control access, as well as disaster recovery plans.

Technical security services: These include processes to protect, control, and monitor information access, such as user IDs, passwords, virus checking, backups, and audit trails.

Technical security mechanisms: These measures aim to prevent unauthorized access to data that is transmitted over a communications network. No specific mechanisms are mandated, but possibilities include secure protocols and encryption.

The administrative procedures and physical safeguards are largely procedural issues rather than technical issues. They overlap with many of the measures included in the Privacy Rule – ensuring that computers are not left logged on when unattended, moving PCs to more isolated areas, etc.

The technical security services and mechanisms focus primarily on patient health information that is stored in computer-based patient record systems. "Paper-to-paper" faxing of patient health information over a phone line is specifically excluded, but e-mailing and faxing of scanned documents over the Internet is not addressed specifically in the rule itself. CEs must take the utmost care when using either of these methods to ensure that personal information cannot be intercepted or compromised.

Complying with the security

The Security Rule gives CEs flexibility in achieving the security objectives and does not mandate specific technologies. Instead, it requires organizations to assess their own security needs and implement appropriate measures to address those requirements. When an organization uses technology in a certain way to reach a specific security objective, then the organization is considered to have complied with the rule.

Faxing and the security rule

Although faxing of information between healthcare-related organizations is very common, any organization that does so must use great care to ensure that they do not violate the HIPAA rules. There are numerous measures CEs can take to comply with HIPAA's Privacy Rule.

These include:

- Keeping fax machines out of public areas
- Designating employees who are authorized to handle patient health information to empty fax trays regularly

The Security Rule, on the other hand, applies only to the electronic transmission of data and specifically excludes "paper-to-paper" faxing over a phone line.3 CEs, therefore, should focus primarily on physical safeguards and procedures to mitigate the risks of sensitive information falling into the wrong hands. These include:

- Verifying the recipient's fax number, notifying them that you are sending a fax, and requesting confirmation of receipt.
- Including a cover sheet indicating that the fax contains confidential health information, it is being faxed with appropriate authorization from the patient, it cannot be re-disclosed without proper authorization, etc., and requesting that it be destroyed if received in error.
- Prohibiting the faxing of highly sensitive personal information (for example, chemical dependency, HIV, mental health, etc.).
- Saving a confirmation sheet or electronic record of the fax transmission, including the date, time, and destination fax number and keeping this with the original record. Objectives and does not mandate specific technologies

When faxing patient health information, eCopy products offer significant advantages over traditional standalone fax machines:

- Integration with fax address lists means you can select the recipient's name, rather than relying on speed dial buttons (easy to press the wrong button) or direct entry of the recipient's number (easy to enter the wrong number).
- When faxing using Microsoft Exchange or Lotus Notes, a copy of the fax is delivered to the sender's inbox or sent items folder. This provides a record of what was sent and to whom.

E-mail and the security rule

When identifiable patient health information is to be exchanged over a public network CEs must take reasonable measures to ensure the confidentiality and integrity of the data. Use of encryption is "encouraged," but so as not to unduly burden small providers, the Security Rule does not actually require its use. Since each CE is responsible for assessing the risk, organizations, especially large ones with multiple locations, may find that internal risks are as great as external risks and therefore choose to encrypt data on the internal network as well. Alternatively, if the information is "de-identified" (enough patient information is removed so that the risk of

identifying the patient is very small) then the information is no longer subject to these requirements. Where a secure local area network or virtual private network is used, encryption is also optional.

eCopy uses file attachments to send scanned documents to e-mail recipients. eCopy's products include optional 128-bit encryption that encrypts attachments before sending them by e-mail. If the document includes identifiable patient health information, encryption is an acceptable way to safeguard the transmission. You enter a password at the point of origin (the eCopy- enabled copier/scanner or eCopy Desktop) and then give the password to the recipient via a safe channel (for example, by phone). The recipient uses this password when opening the attachment to reverse the encryption algorithm. Since encryption is only as strong as the password used to create the encryption key, eCopy recommends using passwords that meet standard secure password guidelines (see your system administrator to inquire about your company's guidelines).

eCopy Desktop also lets you "de-identify" patient health information before sending it over the Internet. eCopy Desktop's markup tools include blackout and whiteout capabilities that let you hide specific sections of the document, for example, the patient's name, address, social security number, or health identifier. These markups can be burned in to prevent the recipient from removing the markups to reveal the underlying information.

The Security Rule also requires audit trails of all electronic transmissions of patient health information. eCopy delivers a copy of the message to the sender's e-mail inbox or Sent Items folder, this can provide a record of the transmission. Additionally, eCopy products log all scanning operations initiated by the attached copier or scanner, providing a detailed audit trail.

Storing scanned documents

Many of the vulnerabilities associated with paper- based patient health information can be reduced or eliminated by moving to electronic document storage. Electronic storage, however, introduces a whole new range of security risks that must be understood and addressed.

Most importantly, adequate security mechanisms must be in place to ensure that only authorized individuals can access the information. Additionally, information must be safe from interception as it is transferred across the network (encryption is not required when information is transferred across a secure local area network or virtual private network, although each organization must make its own risk assessment).

eCopy provides several ways to conveniently store paper-based documents as electronic files:

- Scan to Desktop lets you scan paper documents to your personal scan inbox and retrieve them using eCopy Desktop. From here you can save them to your local hard drive, a network file server, or any one of the many supported document management systems.
- eCopy Quick Connect delivers scanned documents to a network folder or FTP site. It offers versatile file naming, index file creation, and destination options, with no programming required.

With eCopy Quick Connect, records become instantly available to authorized users, and integration of paper-based information into existing patient record systems and workflows becomes automated.

- Optional integration with leading document management systems lets you scan documents into your system directly from your eCopy-enabled digital copier or scanner. The list of supported systems includes Canon imageWARE, EMC Documentum, Hummingbird Enterprise - DM, Interwoven WorkSite, and Open Text's Livelink, plus many others from third party software developers.
- eCopy's Software Developer Kit (SDK) provides the tools needed to scan documents directly into your custom business applications.

Once in electronic form, scanned images are subject to all the administrative, technical, and physical requirements of the Security Rule. eCopy products include several features to facilitate compliance with security requirements:

- With Scan to Desktop, eCopy uses existing operating system security to ensure that only the owner can access his/her inbox. When you retrieve a scanned document from your scan inbox using eCopy Desktop, you must save it to a local hard drive or network server. It is important that the storage location be secure if identifiable patient health information is involved. Note that the same applies if you receive patient health information as an e-mail attachment.
- With eCopy Quick Connect, the administrator can configure the destination folders so that only individuals with authorization to view the patient health information have access. This can be accomplished using existing NTFS or Novell security. If additional security is required, 128-bit document encryption is available.
- Most document management systems provide robust security that determines who has access to which documents. Administrators can configure their systems to provide minimal access to patient health information, with audit trails available to monitor access.

Security Rule

eCopy's document distribution technology can help businesses achieve cost savings and increase organizational efficiency while complying with HIPAA's strict privacy and security requirements. Regulatory requirements and eCopy product features are summarized in the table on the following page.

	HIPPA Requirement	eCopy Product Feature
Confidentiality	Organizations must take all responsible steps to ensure that only authorized individuals see patient health information.	• Electronic distribution of paper-based patient information reduced the possibility of unauthorized access. • Sending information by e-mail rather than fax ensures that it is delivered to a private e-mail inbox rather than a public fax machine. • Main scanning functions require password authentication, restricting the ability of unauthorized users to distribute patient health information. • Optional secure deletion of temporary files at the end of each scanning operation ensures that files are purged by overwriting the disk locations multiple times with random characters.
Auditing	Organizations must maintain a record of patient health information disclosures.	• A copy of the sent e-mail or fax is delivered to the sender's inbox or sent items folder. • eCopy maintains a transaction log of all scanning activity.

	HIPPA Requirement	eCopy Product Feature
Minimum Disclosure	Disclosure of patient health information should be limited to the amount of reasonably necessary to accomplish the intended purpose.	• Drag-and-drop e-mail and fax capability lets you select which pages of the patient's record to send. • Markup tools let you "whiteout" or "blackout" personal information before delivering it to a third party.
Encryption	Identifiable patient health information sent over a network must be safeguarded	• Optional 128-bit document encryption of file attachments help patient health information remain confidential.
Authorization	Computer system users must only have access to information they are authorized to see.	• Operating system security ensures that only authorized individuals can retrieve documents from scan inbox. • Users can store scanned documents on a secure NTFS partition or network file server with appropriate access controls. • Integration with major document management systems lets organizations with such systems extend access controls to scanned paper documents. • Users are authenticated at the scanning device before any patient information is sent over a public or private network.
Disaster Recovery	Organizations must implement physical safeguards to protect systems storing patient health information from fire and other hazards.	• Scanned documents can be backed up to an offsite location
Availability	Patient health information must be readily available to authorized persons within an organization	• Scanned documents are available for instant access by authorized users. • Immediate transfer of paper documents between internal departments can be done in several ways: - E-mail or fax the documents with eCopy, eCopy Quick Connect can be configured to deliver documents to a secure department storage location, Scanned paper documents can be made searchable using eCopy's built-in OCR functionality

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.
ONE WAYSIDE ROAD
BURLINGTON, MA 01803
781 565 5000
NUANCE.COM

NUANCE